A QUANTITATIVE RISK ANALYSIS MODEL FOR PRIVATE SECURITY MANAGERS

by

GABRIëL JACOBUS LE ROUX

Submitted in accordance with the requirements

for the degree of

DOCTOR OF LITERATURE AND PHILOSOPHY

in the subject

POLICE SCIENCE

at the

UNIVERSITY OF SOUTH AFRICA

PROMOTER: PROF C W MARAIS

JUNE 2004

STATEMENT

I declare that " A Quantitative Risk Analysis Model For The Private Security Managers" is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

G. J. LE ROUX

Dedicated to my wife, Nettie le Roux, for her inspiration, dedication and confidence in me.

PREFACE

I thank God the almighty for his grace during the course of these studies.

I want to express my appreciation towards my supervisor Prof. Coen Marais for his patience, insight and guidance.

To my lovely wife, Nettie, thank you for your support during all my years of studying. Without your support and faith I wouldn't have reached and fulfilled this dream. This book is dedicated to you as the fruit of your constant encouragement and support.

To my lovely children Heinrick, Lisa, Jacques and Jolette for their constant faith in me. Thank You.

To Dirk Paulsen, I have no words for this great mentor. His encouragement and support during my studies, which started in 1983, speaks volumes. Thank You.

My appreciation to Carel Barnard for inviting me to Media24 conferences and the part he played in the developing of this model.

A special thanks to Johann de Meyer for his advice, input and assistance regarding the quantitative issues in this study.

To Leon, my brother, your support and encouragement didn't go unnoticed. Thank You.

To all my friends and colleagues who served with me at Atlas Aircraft Corporation where my studies originated, and who also support me in achieving the highest qualification.

All participants during the testing of my model. Thank You.

Finally, my most sincere appreciation to Jacques and Jolette, who I believe, sometimes neglected their two children, to spend long hours at their computer to complete this manuscript.

NUMBERING AND REFERENCE SYSTEM

NUMBERING OF CHAPTERS AND SUBDIVISIONS

1. -CHAPTER NUMBER
1.1. -SECTION HEADING
1.1.1. -Subsection heading
1.1.1.1 -Sub-subsection heading
1.1.1.1.1 -Lists in sections

or a - Numbered lists in sections

- Page numbers per chapter

A-1 - Page numbers per appendix

REFERENCE SYSTEM IN THE THESIS

The Harvard classification system has been used throughout the study. Where the text refers to an author, the reader will find the source in the alphabetical lists in the Bibliography Appendix.

Where necessary, footnotes were used for further reference clarification.

Articles obtained from the Internet are not numbered according to the page references normally found in documents. The researcher therefore included the specific electronic file, along with the information referred to, in footnotes.

The bibliography includes:

- Books
- Magazine articles
- Articles and organizational homepages on the Internet

- Theses, essays and research reports
- Security documents
- Pamphlets.

USE OF ABBREVIATIONS

Abbreviations are used after they have been explained.

p. and pp. are used throughout the text to indicate page numbers.

OTHER APPLICATIONS

The male person is used to simplify reading of the document.

SUMMARY

A QUANTITATIVE RISK ANALYSIS MODEL FOR PRIVATE SECURITY MANAGERS

by

GABRIëL JACOBUS LE ROUX

DEGREE: DOCTOR OF LITERATURE AND PHILOSOPHY

in the subject

POLICE SCIENCE

PROMOTER: PROF C W MARAIS

An easy-to-use quantitative risk analysis model is developed for the private security industry in South Africa, which can be used as a suitable analysing tool in the hands of the private security manager.

This model incorporate different concepts such as the probability, impact, cost of risk, degree of correction and the newly established human factor concept, which cannot be seen in isolation. This latter concept plays a major part in the overall risk quantification process in establishing a most accurate risk score rating.

The human factor concept, also known as the "CHHP" approach, is the first concept, which will round the model of in an effective measuring way. Human factors such as (i) control measures (ii) human attitude towards the risk (iii) handling of the risk and (iv) understanding and implementation of policies and procedures are combined to form part of the total integrated quantitative risk analysis model, also known as the "TIQCAM"-model.

The "TIQCAM"-model uses Excel spreadsheet format as the principal means to illustrate the total integration of all risk concepts and also providing the user of the model with a solid foundation in analyze physical and quantifiable security risks. This model will also enable the user to use it as a value-added service to their clients.

Keywords:

Quantitative; Analysis; Risk; Modelling; Management; Private security; Managers, Mathematics; Concepts; Risk classification.

OPSOMMING

A QUANTITATIVE RISK ANALYSIS MODEL FOR PRIVATE SECURITY MANAGERS

deur

GABRIëL JACOBUS LE ROUX

GRAAD: DOCTOR LITERATURE AND PHILOSOPHY

In die

POLISIE WETENSKAP

PROMOTOR : PROF C W MARAIS

‘n Gebruikers-vriendelike kwantitatiewe risiko analise model is ontwerp vir die Suid-Afrikaanse privaat sekuriteitsbedryf , wat die sekuriteitsbestuurder met gemak kan gebruik vir analise doeleindes.

Hierdie model inkorporeer verskillende konsepte soos die waarskynlikheid, impak, risiko koste, graad van korreksie en die nuwe menslikheidsfaktor konsep, wat nie in isolasie beskou kan word nie. Laasgenoemde konsep speel ‘n fundamentele rol in die algehele kwantitatiewe risiko analise proses wanneer gepoog word om die mees akurate risiko te bepaal.

Die menslikheidsfaktor konsep, ook bekend as die “CHHP”-benadering, is die eerste konsep wat die model sal afrond tot ‘n effektiewe maatstaf. Menslike faktore soos (i) kontrole maatreëls (ii) menslike ingesteldheid tot risiko (iii) hantering van risiko en (iv) insig in en implementasie van beleide en prosedures word gekombineer om deel te vorm van die totale geïntegreerde kwantitatiewe risiko analise model, ook bekend as die “TIQCAM”-model.

Die “TIQCAM”-model maak gebruik van ‘n Excel werkboek formaat om die totale integrasie van alle risiko konsepte te vertoon en voorsien die gebruiker ook van ‘n vaste grondslag vir die analise van fisiese en kwantifiseerbare risikos. Hierdie model sal ook die gebruiker in staat stel om ‘n toegevoegde waarde diens aan kliënte te bied.

TABLE OF CONTENT

PAGE

LIST OF TABLES

PAGE

LIST OF FIGURES

PAGE

CHAPTER 1

GENERAL ORIENTATION

1.1 INTRODUCTION

Businesses have been using mathematical[1] tools to help solve problems for thousands of years. The formal study and applicability of quantitative techniques to practical decision making is, however, largely a product of the twentieth century. The techniques in this study can be applied successfully to an increasingly wide variety of complex problems in business, government, education, security and safety, and many other areas.

It isn't enough, though, just to know the mathematics of how a particular quantitative technique works; you must also be familiar with the limitations, assumptions, and specific applicability of the technique. The successful use of quantitative techniques usually results in a solution that is timely, accurate, flexible, economical, reliable, and easy to understand and use.

1.2 PROBLEM STATEMENT

The researcher has, in the course of his research for his Master's Degree with regard to the "Posisionering van Risikobestuur binne Naspers" came to the conclusion that managers neither possess the knowledge nor the skills needed for risk management (Le Roux 2000: 187). This results in a lack of necessary care and seriousness when approaching the risk situation. Taking this into consideration, the primary problem with private security managers seems to be the ignorance with regard to the nature, extent, as well as content of risk management, and more specifically the analysing thereof.

An analysis of the primary problem indicates the following secondary problems:

---

1 Mathematical model is a set of mathematical relationships that represent, or approximate, a real situation (Wayne & Albright 1997:4).

- The first secondary problem appears to be the lack of an effective quantitative risk analysis model for private security managers, which can be used successfully to identify and control risks within the organizational environment.

- The next secondary problem is the need for security managers to know how to use a suitable quantitative risk analysis model, thereby bringing about an effective analysis of the physical risk facing companies where security service is rendered.

Except for the secondary problems, it is found that a quantitative decision-making model exists on short-term crime prevention measures (Roelofse 2001:i). Although this model integrates some of the concepts, it does not employ any human factors, which is one of the important concepts in the researcher's "TIQCAM" model.

Roelofse (2001:26) further states that the decision-making model forms the crux of his thesis. Researcher's model is directed towards the security industry to supply them with a software tool in measuring risk and to set a risk classification of high, medium or low, which can then be taken in consideration during the decision-making process.

Research as opposed to inquiries are also done at international level, which indicate that a quantitative risk analysis model does not exist for the security manager (see schedules B and C). Inquiries done at Security Industry Regulatory Authority (SIRA) also indicate that no training material or other literature exist in quantitative risk analysis for security managers.

This motivated the researcher to develop a suitable model for the private security industry in South Africa.

It must be stated that the researcher design his own model, which was called "FAMASER" (Facility Management Services)[2]. By testing this model it was found by the delegates (selected group of security managers), that it is problematic in the sense

---

[2] *See point 1.5.3.4(Pre-testing of quantitative risk analysis model).*

that the model is too complicated to use. An Easy-To-Use Model is suggested which leads to this research in developing a convenient model.

Having thus stated the problem, the objective of the research will now be formulated.

1.3 RESEARCH OBJECTIVE

The objective of the research is formulated as a result of stating the problem, and therefore provides the angle from which the research is done. The objective of the research is to provide the South African private security managers with guidelines in using a quantitative risk analysis model.

This objective includes the following:

- To determine the exact need within the private security industry in developing a quantitative risk analysis model.

- To carry out a theoretical investigation with regard to quantitative risk analysis models on a national level in order to ascertain what its didactic-scientific foundation should be.

- To establish guidelines for the development of a risk analysis model for private security managers for not only analysing risk in their own environment, but also use it as a value-added service to their clients. In the process, attention should be given to the structuring of a physical risk analysis model to ensure the meaningful implementation thereof.

- The objective is also to supply security managers with the essential skills and knowledge they need to make their own decisions with regard to the seriousness of physical risks when using the quantitative risk analysis model.

It should be mentioned that since training methods in a business context are normally coordinated by human resources, it becomes the responsibility of the organization's

management to care for the development of human resources, meaning staff as well as managers in a wide variety of fields, such as transport, marketing, health and safety and many other areas. The total spectrum of risk management is a specialised field of expertise and would therefore not be typified as a human resources function. The development of a quantitative model in risk analysis (a risk management function) can inevitably also involve the human resources trainers, who, in turn, can train managers in the their different areas.

Although the model can be a helpful tool for training purposes, the main contribution by the researcher in this study is to utilise a mathematical configuration (natural/pure science) to create a basic social science model.

1.4 RESEARCH HYPOTHESIS

The following hypotheses are formulated with the eye on the subject and against the background of the foresaid research objectives and goals.

The researcher believes that:

Hypothesis 1 - No practical quantitative risk analysis model exists in South Africa's private security companies

Hypothesis 2- The private security managers are unskilled in quantitative risk analysis

After researching the abovementioned hypotheses, the researcher will conclude that no quantitative risk analysis model exists for the private security industry and that the security manager is in fact unskilled in the use thereof. It must be noted that the concentration will therefore be solely on the development of a physical[3] quantitative risk analysis model for the private security manager.

[3] *See discussion under point 1.5.1.2, the last paragraph, for more insight regarding the physical aspect*

1.5 RESEARCH METHODOLOGY

The following aspects will be dealt with, which is of vital importance for this study:

1.5.1 Demarcation

1.5.1.1 Spatial

The research involved fifty (50) security managers from seven (7) different security companies on a national basis in the Republic of South Africa. Two regions were selected for this research project, namely the Western Cape and Gauteng. The reason for this is that the seven selected security companies are mostly situated and operative in both these regions.

Two groups of managers were also present, namely: (i) security managers, and (ii) risk practitioners. Referring to the last group it is found that some security companies have their own perception of the term “Risk Practitioners” or “Risk Manager”. For those companies the foresaid terms still refer to the security manager. The reason for this is that the risk practitioner and/or risk manager is also responsible for the total spectrum of physical security. For the purpose of this research project, the researcher will mostly use the term “Security Manager”.

Researcher must highlight the point that although the three-step career part of management (See table 2.1) establishes the steps as (i) junior management (ii) middle management and (iii) senior management, the focus was between middle and senior management. For the purpose of this study, where the fifty (50) security managers were involved as the research group, the researcher shall only abide

by the term “Security Managers” whether they are junior, middle or senior management.

1.5.1.2 Concept demarcation

In doing a risk analysis, all the different risk analysis concepts are taken into consideration. These concepts have their own criteria, indicator and risk rating, which is important in the analysing process to come to a positive result regarding the risk problem.

These concepts are illustrated in the following steps:

- Step 1: Probability
- Step 2: Impact
- Step 3: Cost factor
- Step 4: Degree of Correction
- Step 5: Human Factor.

After all the steps are taken into consideration, it will then reflect the risk subtotal and the risk total where after a risk classification will be established. This classification plays a fundamental role in the whole analysing process because it will then determine if future action is needed. This also means that the future action must then be taken into consideration for decision-making purposes in solving the risk problem. The future action is illustrated with a red connection to place the emphasis on the importance of solving the risk problem (see figure 1.1 under 1.6.3).

Furthermore the researcher will only use two physical risk problems, namely robbery and fraud, as an example to establish the end result of that spesific risk problem by using the different concepts as mentioned. Hypothetical ratings will be assigned to the two above mentioned risk problems in order to come to a final risk

classification. This will give the reader a better insight in how to use the model in a practical way.

1.5.1.3 Quantitative and qualitative approaches

A brief explanation to elucidate the difference between qualitative and quantitative research is necessary to ensure that the reader understand the terms and is able to bring in into context with this research study.

Babbie (1992:372) describes qualitative data as non-numerical data and quantitative data as numerical data. He further differentiates between these terms as follows:

(i) **Quantitative research -** quantification ensures that observations are more explicit and therefore makes it easier to accumulate and summarise data (statistical analysis) i.e. collecting data in the form of numbers.

(ii) **Qualitative research -** qualitative data is richer in meaning, although the qualitative researcher has less control mechanisms. This means that the researcher will be more involved with observation and fieldwork i.e. data collected in the form of words or pictures (Neser, Joubert & Sonnekus, 1995:182).

(iii) **Triangulation as a combination of the quantitative and qualitative approaches**

After a preliminary literature study in 2001, the researcher started his research in 2002, and decided to utilize a combination of the quantitative and qualitative approaches, which is called the triangulation approach. An information schedule is used in order to establish the need for a

quantitative risk analysis model for private security managers (see sample information schedule as schedule “A” and discussion under 1.5.3.3).

The reason why researcher chose the triangulation approach for this study, is that it enables deeper understanding of this research, by combining the methods.

De Vos (2002:342) advocates that there are several types of triangulation of which triangulation of methods means mixing quantitative and qualitative styles of research and data. This study is carried out by using two methods in parallel, or both simultaneously.

Patten (2002:247) places the emphasis strongly on the use of the triangulation approach by stating that combining methods also strengthens a study. This can mean using several kinds of methods or data, including using both quantitative and qualitative approaches.

According to Healy and Perry (in Golafshani 2003:603) argue the involvement of triangulation of several data sources and their interpretations with those multiple perceptions in the realism paradigm. Some scholars at the University of British Columbia, Canada, also argue that quantitative and qualitative approaches should not be triangulated. They believe that using mixed methods is method slurring and consider it to be sloppy research (Hilton 2002:3).

Researcher is of the opinion that any individual is entitled to his own perception, however the researcher’s perception is that using the triangulation approach in this study, can only provide confirmation and completeness. De Vos (2002:242)

adds that it also allows researchers to be more confident of their results.

1.5.2 Research techniques

The research methodology can be described as:

- Descriptive
- Interpretive
- Application

(i) Descriptive

Research has various shapes and sizes and it is therefore necessary that the researcher decides on the type of research that he intends doing, prior to the start of his study (Neuman, 1997:18).

This study is focussed on the researcher's contribution to the science of policing (security) and therefore it is imperative for the researcher to pursue levels of descriptive, interpretation and application.

It is also important to differentiate between the different types of studies (Mouton & Marais, 1991:42) and to indicate which study or combination of studies will be applicable to this research study.

The three types of studies are:

- **Exploratory Studies** - The goal of exploratory studies is the exploration of something new or about a relatively unknown area (Mouton & Marais, 1991:43) of which the investigator has little or no knowledge about. Neuman (1997:19) explains this type of study as a relatively new topic or issue in which the researcher tends to address the "what" question.

- **Descriptive Studies -** Descriptive studies are more specific with its main aim to observe and report on events or actions. According to Neuman (1997:20) this type of study represents a great deal of social research and focus on the "who" and "how" questions. The researcher therefore conducts his/her research to describe the subject and to provide a detailed picture thereof.

- **Explanatory Studies -** The aim of explanatory studies is to explain a given phenomena in terms of specific causes (Marais & Mouton, 1991:45) i.e. the desire to know "why" (Neuman, 1997:20).

Taking the abovementioned descriptive discussion in perspective, it should describe any situation or area of interest, factually and accurately.

(ii) Interpretive

The researcher's view of "interpretive" is that data is gathered (See point 1.5.3.1) that generates "thick" description and interpretation that allows theory building. This study will include the researcher's interpretation of the quantitative risk analysis model for the private security manager.

(iii) Application

Although an investigation of this nature will inevitably lean towards the philosophical, and even the normative, an effort will be made to concentrate more on the practical application, in that the researcher's own experience in risk management will be used to supplement the manuscript study. Informal conversations with fellow researchers, trainers and academics at universities and technikons will similarly serve to support and confirm the researcher's experiences and opinions.

The abovementioned discussion is also applicable when collecting data for this research project (See point 1.5.3.1).

1.5.3 Research procedure

1.5.3.1 Data Collection

Fundamental to this research is data collection. It refers to the survey methods that will be developed and utilized to obtain information. The methods utilized relevant to this project are literature studies whereby the researcher will utilize journals, books, Government documents, policy reports, presented papers and the internet. This method is of an empirical nature because mathematics (numbers) forms part of this study.

Glazer (2001: 1) defines empirical study as study that includes a brief review of the literature, a research question or hypothesis, hard (numbers) data from a group of participants in a study, a statistical result section, and discussion section of the results.

It must be stated that the researcher's own experience of risk management, National Key Points and big companies, who are investing a lot in security measures in protecting their personnel, assets and properties, will also be used to supplement this study (see last paragraph under point 1.5.2 – (iii) application).

1.5.3.2 Sampling

According to Du Plooy (2001:16) the following sampling techniques exist:

- Probability samples

- Simple random sample
- Stratified random sample

- Quasi-probability samples
  - Systematic random sample
  - Cluster random sample
  - Multi stage random sample

- Non-probability samples
  - Convenience sample (Sometimes called accident, available or opportunity sample)
  - Purposive sample (Known-group/judgement or quota sample)
  - Volunteer sample
  - Snowball sample

The researcher selects his own sampling technique and respondents, which is based on the **"purposive sampling technique".** According to Huysamen (1994:44) this is the most important kind of non-probability sampling. Researchers rely on their experience, ingenuity and/or previous research findings to deliberately obtain participants in such a manner that the sample obtained may be regarded as representative of the relevant population.

In order to establish the size of the research group the viewpoint is that it should be proportional representative of the universum. The perception also exists that it is not the size of the research group that determine the reliability, but rather if the research group is representative of the universum (Van Vuuren, 1992:9).

Researcher also agrees with Van Vuuren (1992:9) that no guarantee can be given that the representative group are in all respects representative of the whole security community or that the results will stay unchanged unless the security community is involved with this

investigation. It can well be said that the representative group is probably accurately representative.

The universum and/or population sample of the researcher consist of the security community in South Africa, which consists of 4,256 security companies (See table 2.2- registered security providers per region). The researcher decides on the top 20 security companies as his research group to be representative of the universum (See Table 1.1).

Table 1.1: Top 20 ranking service providers

Ranking	Service Provider	Employees	Industry %
1	FIDELITY SECURITY SERVICES	18,445	8.43%
2	SECURICOR GRAY SECURITY SERVICES	9,263	4.24%
3	CALLGUARD & SUBSIDIARIES	8,295	3.79%
4	MAGNUM SHIELD SECURITY	6,853	3.13%
5	CHUBB & SUPERGROUP BBR	6,691	3.06%
6	COIN SECURITY GROUP	4,250	1.94%
7	ADT& SENTRY	4,110	1.88%
8	SECURECO (PTY) LTD	3,791	1.73%
9	ENFORCE GUARDING (PTY) LTD	2,698	1.23%
10	COMMAND SECURITY SERVICES	2,206	1.01%
11	MAXI SECURITY 2000 (PTY) LTD	1,951	0.89%
12	PROTEA SECURITY SERVICES	1,663	0.76%
13	GREMICK- A DIVISION OF SERVEST	1,613	0.74%
14	STALLION SECURITY (PTY) LTD	1,502	0.69%
15	DE BRUIN SECURITY CC	1,315	0.60%
16	GONDO SECURITY SERVICES	1,234	0.56%
17	PEACEFORCE SECURITY CC	1,163	0.53%
18	BHEJANE SECURITY CONSULTANTS	1,125	0.51%
19	HLANGANANI PROTECTION SERVICES	1,120	0.51%
20	LODGE SERVICES (PTY) LTD	1,080	0.49%

Source: Private Security Industry Regulatory Authority

The researcher puts all the names of the top 20 security companies in a hat and drew four names, which now form part of this research project (See table 1.2).

Table 1.2: Informal survey for the need of developing a quantitative risk analysis model for security managers

Security Providers	**% Need of**	**% Not in need of**
NASAP (National Strategic Asset Protection)	100%	0%
ASAP (Atlantis Security Asset Protection)	92%	8%
Group 4 Security Services	83%	17%
Company A (Listing top 20 company)	100%	0%
Company B (Listing top 20 company)	75%	25%
Company C (Listing top 20 company)	83%	17%
Company D (Listing top 20 company)	92%	8%

Source: Own compilation

From this universum three (3) other security companies were also identified. The representative group as per figure 1.2 are in total seven (7) security companies, thus the sample representing the security community.

It must be clearly stated, that no reference was made regarding Companies A – D (see table 1.2), due to a request that their business and interviewers identity must be handled strictly confidential.

1.5.3.3 Information Schedule

Groenewald (1988:44) states that research interviews are a conversation with the aim to obtain information. This conversation

can range from an informal or unstructured to a formal or structured interview and can take place with or without an accompanying questionnaire. Bailey (1987:106) is of the opinion that an instrument that is not given directly to the respondent but is filled in by an interviewer who reads the questions to the respondent is generally called an interview schedule.

The researcher made use of an information schedule, which gave rise to individual interviews with security managers in seven different private security companies, four of which are listed as the top 20 security companies in South Africa (See Table 1.1). Affirmative notes of the interviews are available with the researcher on demand considering the identity of persons involved has been handled as strictly confidential.

The information schedule that is used contains 12 main questions with 50 sub-questions. The purpose of this schedule is to gather information to establish the need for developing a quantitative risk analysis model for security managers in South Africa.

The researcher selected negative answers from the information schedule by marking them with a red symbol called asterisk, which indicates that the more negative answers is marked, the more companies are in need of a quantitative risk analysis model.

The two main leading questions asked in the information schedule (see schedule "A") leads to the formation of statistics (See Table 1.1) in discovering the need for the development of a quantitative risk analysis model for private security managers. The following two questions were taken into consideration when formulating the needs survey.

- How is risk analysis defined in your organization?

- To what degree is risk analysis, accepted by management?

The calculations in the information schedule were solely worked on the negative rating. The amount of scores achieved as a negative answer is divided by the 12 questions (See information schedule A) and then multiplied it by 100 to change it to percentage. The higher the negative percentage the more the companies are in need of a quantitative risk analysis model (See table 1.3 for calculations)

Table 1.3: Calculations according to information schedule

Security providers	**Negative calculation**	**%**
Nasap (National Strategic Asset Protection)	12 / 12 x 100	100
Asap (Atlantis Security Asset Protection)	11 / 12 x 100	92
Group 4 Security Services	10 / 12 x 100	83
Company A (One of Top 20)	12 / 12 x 100	100
Company B (One of Top 20)	9 / 12 x 100	75
Company C (One of Top 20)	10 / 12 x 100	83
Company D (One of Top 20)	11 / 12 x 100	92

Source: Own compilation

According to the percentage not in need of a quantitative risk analysis model to be developed, it is not that the respondents are negative in this regard, but they rather do not perceive it as necessary, due to the fact that they are physical security providers and not risk analysts.

It is also important to establish whether the abovementioned instrument (information schedule) is trustworthy and accurate, which must be taken in consideration when measuring the validity and reliability of measurement.

According to Bailey (1987:66) the definition of validity has to parts:

(1) that the measuring instrument is actually measuring the concept in question, and not some other concept; and (2) that the concept is being measured accurately. Both Van Vuuren (1992:14) and Groenewald (1988:30) agree but the latter is of the opinion that validity should also be transformed to the ability of the researcher in carrying out the process of measuring in a consequent manner.

The validity of the researcher's information schedule is tested on the hand of personal interviews (see Appendix A) as well as a presentation to various security managers (see pre-testing under point 1.5.3.4). The test can therefore be viewed as reasonably trustworthy and reliable, because it happens to test what should be tested, namely, the importance of relevant questions, the way in which the questions are asked and understood.

Concerning the reliability, it must also measure what it is supposed to measure (Van Vuuren 1992:15-16). Although the two essential measuring instruments, the Alpha and Cronbach coëffisiënt, ensure the most reliable and accurate outcome according to Bohrnstedt in Van Vuuren (1992:15-16), the researcher is of the opinion that the validity and reliability in his measuring process is accurate and ensure not only consistency, but that the respondents are convinced that all the questions in the information schedule are relevant to the stated goals of this study.

1.5.3.4 Pre-testing of quantitative risk analysis model

Pre-testing is the final stage in questionnaire construction and one of the most important (Bailey 1987:141). The sample for a pre-test is usually some "captive audience" such as office staff, co-workers, fellow students or family (Bailey 1987:141).

The researcher also pre-tested the quantitative risk model, by using Excel spreadsheets, which were developed and a presentation in this regard was held in Cape Town. Various security managers and risk practitioners attended this presentation. Two types of quantitative risk analysis models were presented.

The first model, called “FAMASER" analysis model”[4] contains all the aspects that are necessary to come to a conclusion in taking a decision in handling risks. The aspects include the probability, impact (severity and sensitivity), cost factor, and degree of correction and researcher’s own viewpoint on human factors. The human factors mainly looks at personnel skills, their attitude to the risk, procedure in handling risk and the emergency aspects regarding their knowledge of the total emergency situation. The conference delegates accepted this quantitative model but the perception is that intensive training should be given, not only to security managers, but also their deputies. With an in-depth discussion whether this model is suitable for security supervisors, all the delegates were of the opinion that they would find it difficult in using the model unless intensive training on the whole aspect of quantitative analysis is given.

A second quantitative risk analysis model was developed solely for the purpose of a more user friendly model for security supervisors, which the delegates received with open arms and their views are that this model is even suitable for use by security managers. This easy-to-use model is only based on human factor questions in a risk situation, which plays a fundamental role in quantifying risks. The following questions are applicable:

- The possibility that a risk might occur;
- The history;
- Circumstances;

[4] *See discussion in Chapter 1 under point 1.2*

- Human factors (skills, attitude etc.);
- Handling of the risk;
- Company procedures regarding the risk.

Although the delegates were impressed and satisfied with both models and view this as a breakthrough for the security managers, it is the perception of researcher that it only gives an indication of the risk rating, whether it is a high, medium or a low risk. It is not really reliable in the sense that no probability or impact factors were considered. This model is taken as the basis where upon the "TIQCAM" model (Total Integrated Quantitative Concept Analysis Model) is developed (See point 1.6.3).

1.6 CONCEPT CLARIFICATION

The following essential terms, which are representative in this study, will briefly be discussed thus providing a better insight and understanding for the reader. Other less important terms that might be applicable are defined in chapter 2 under point 2.2. Also considering the fact that many authors have different views of the terms that's been defined, the researcher is going to abide by the author's definitions as mentioned.

1.6.1 Risk

Risk is associated with virtually every activity one can think of, but according to Ozier (2003a: 5) risk is defined as the chance or likelihood of an undesirable event occurring and causing harm or loss. The key element of risk here is uncertainty, without which there is no "risk".

For the purpose of this study, researcher shall limit the meaning of the word *"risk"* to the uncertainty of financial loss, the variations between actual and expected results, or the probability that a loss can occur or will occur. This means that quantitative concepts, such as probability, impact (involving

sensitivity or severity), cost factor, degree of correction and human factors, play a fundamental role in any risk situation and in the establishment of risk classifications, whether it is high, medium or low.

Risk quantification and using concepts are fundamental to the main business of any organisation. Risks in business context is normally of a physical nature and is seen as non-speculative that have no potential for showing profit (Valsamakis, Vivian & Du Toit 2000:36).

Broder (2000:5) also places a high priority on the so-called physical risks in business. The following events or kinds of risk are the most commonly concerned:

- Natural catastrophe (tornado, hurricane, seismic activity);
- Industrial disaster (explosion, chemical spill, structural collapse, fire);
- Civil disturbance (sabotage, labour violence, bomb threats);
- Criminality (robbery, burglary, pilferage, embezzlement, fraud, internal theft, hijacking);
- Conflicts of interest (kickbacks, trading on inside information, commercial bribery, other unethical business practices).

All the risks in both of these categories are likely to need particular, individual attention when analyzing the overall “riskiness”. A decision must be made about which risks are amenable to more detailed evaluation and quantification (Martin & Tate 2002:4).

Researcher is of the opinion that the security science can play a more prominent role in assisting the business community in quantifying their physical risk.

1.6.2 Risk Analysis

According to Shimonski (2002:2) risk analysis is also known as risk assessment and is becoming more and more untenable in terms of usability, flexibility, and critically in terms of what they produce for the user. Ozier (2003a:5) disagrees with Shimonski on the fact that risk analysis and risk assessment are one concept. According to Ozier (2003a:5) it is totally two different concepts and must be handled accordingly. The latter author's version of risk analysis is the process of gathering and analysing risk-related information in the preparation of a risk assessment. Risk assessment is a rather detailed articulation of the risks associated with the information assets and supporting resources at risk, threats that could adversely impact those assets, and vulnerabilities that could allow those threats to occur with greater frequency or impact (Ozier 2003a:5).

Broder (2000:2) is of the opinion that risk analysis is a management tool, the standards for which are determined by whatever management decides it wants to accept in terms of actual loss. Valsamakis, Vivian and Du Toit (2000:26) refer to risk evaluation as the analysis of loss exposure, where attention is focused on how frequent and how severe accidents are likely to be and how they may interfere with the organization's success. In other words, risk analysis entails quantifying the risk and determining its possible impact on an organization. With this in mind quantitative analysis can therefore be defined as the scientific approach using quantitative techniques as a tool in decision-making. A briefer discussion on what quantitative risk analysis implies will follow in chapter 2 under point 2.2.6.

To promote unity of thought, "Risk Analysis" instead of " Risk Assessment" will be used throughout this study.

1.6.3 Model

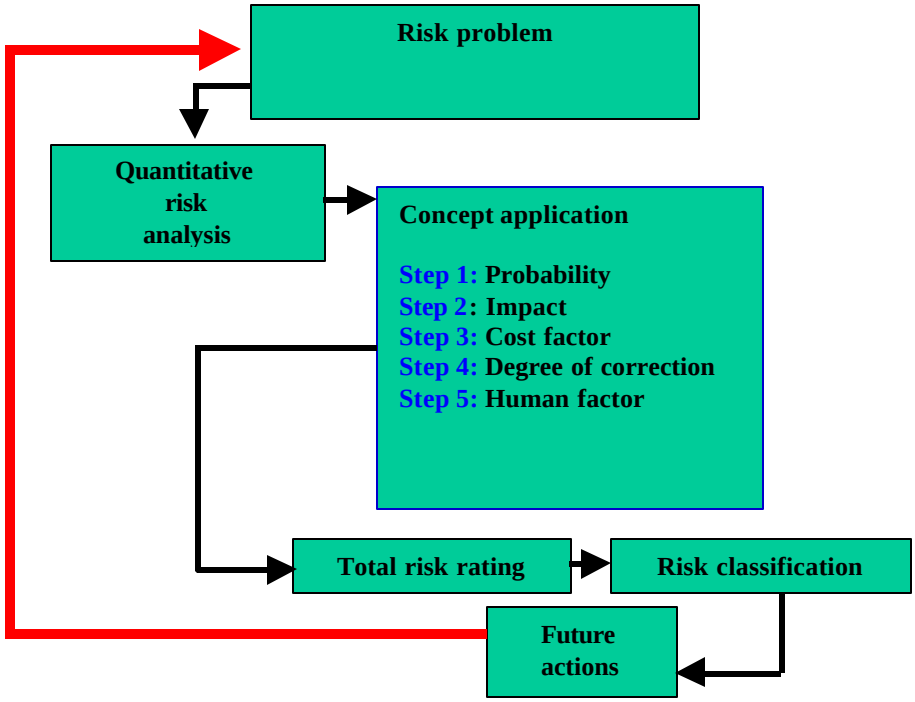
Although there are many views about the definition of the term model such as the representation of reality or real life situation, the perspective of Koller (2000:6) is that the model be a spreadsheet that has taken the leap from being a data organizer to an analysis tool. A model thus represents a process with combinations of data, formulas and functions. By adding cells that help you better understand and analyse your data, your data spreadsheet becomes a spreadsheet model.

For the researcher the focus in this study would be on a mathematical model. This means a model following a quantitative approach by using mathematical equations and concepts to represent the relationship within the model. These concepts, namely: probability, impact, cost factor, degree of correction and the human factor (See chapters 3 to 7) will then be integrated in establishing the full potential of the model by accurately setting the risk classification, which are solely based on physical (crime-related) risks. The researcher's model will be a spreadsheet that will take the leap as an analysis tool, which will then be called the "TIQCAM" model as illustrated in figure 1.1.

The model is a flow chart process, integrating all the quantitative concepts that will be made applicable in the developing of the model.

The "TIQCAM" model starts off with a risk problem, which will lead to the commencement of a quantitative risk analysis. In doing a risk analysis, the analyst should take all the different concepts into consideration. These concepts have their own criteria, which are important in the analysis process to come to a positive result regarding the risk problem.

Figure 1.1: Total integrated quantitative concept approach model



Source: Own compilation

1.6.4 Mathematics

According to authors Levey and Greenhall (1985:1094) mathematics is a deductive study of numbers, geometry and various abstract constructs.

Mathematics is very broadly divided into foundation, algebra, analysis, geometry and applied mathematics. The term "applied mathematics" loosely designates a wide range of studies with significant current use in the empirical science. It includes computer science, mathematical physics, probability theory and mathematical statistics.

Reksnes (2003: 4) is also of the opinion that the terms "mathematics" and "quantitative" represent the same purpose. Both deal with numbers, functions, and the sequence theories. A brief discussion on the latter aspects follows:

1.6.4.1 Number theory

A branch of mathematics concerned with the properties of the integers (the numbers 0, 1, -1, 2, -2). Modern number theory made its first great advances through the work of Leonhard Euler.[5] Most of the focus is on the analysis of prime numbers, i.e., those integers *p* greater than 1 that are divisible only by 1 and *p*; the first few primes are 2, 3, 5, 7, 11, 13, 17 and 19. The fundamental theorem of arithmetic asserts is that any positive integer *a* is a product of primes that are unique, except for the order in which they are listed. For example, the number 20 is uniquely the product of 2x2x5 (Levey & Greenhall 1985:1094).

1.6.4.2 Function theory

The function theory in mathematics is described as a relation that assigns to each member *x* of some set X (the domain) a unique member *y* of some set Y (the range); y is said to be a function of *x*, usually denoted *f* (*x*) (read "*f* of *x*"). In the equation *y* = *f* (*x*), *x* is called the independent variable and y the dependent variable. Although a function *f* assigns a unique *y* to each *x*, several *x's* may yield the same y; e.g., if *y* = *f* (*x*) = *x* 2 (where *x* is a number), then *f* (2) = *f* (- 2) = 4. If this never occurs, then f is called a one-to-one, or injunctive, function (Levey & Greenhall 1985:1095).

1.6.4.3 Sequence Theory

Authors such as Levey and Greenhall (1985:1095) describe sequence in mathematics as an ordered set of mathematical quantities, called terms. A sequence can be finite, like 1, 2, 3, …50, which has 50

[5] *Leonhard, Euler (1707-83) Swiss mathematician. The most prolific mathematician who ever lived, he worked at the St. Petersburg Academy of Science in Russia and at the Berlyn Academy. He contributed to areas of both pure and applied mathematics, including calculus, analysis, and number theory.*

terms, or infinite, like 1, 2, 3, …, which has no final term. An infinite sequence may or may not have a limit. Frequently there is a rule for determining the terms in the sequence, as in the Fibonacci [6]sequence and in various types of progressions.

Although the term "Mathematics" and "Quantitative" represent the same meaning, researcher will use both terms to make sense in the contexts it is been used.

1.6.5 Statistics

Statistics is a branch of applied mathematics dealing with the collection and classification of data by numerical characteristics and the use of these data to make inferences and predictions in uncertain situations. Generally, measurements taken from a small group, the sample, are used to infer the behaviour of a larger group, the population, as in television ratings and election predictions. The theory of probability is necessary to determine how well the sample represents the population. Statistics is used in scientific and social research, insurance and many other fields (Levey & Greenhall 1985: 1096).

1.6.6 Probability

Render et al (2003:34) describe probability as a numerical statement about the chance that an event will occur. According to Le Roux (2002: 7) probability measures the likelihood that an event will occur. Both definitions are of a mathematical nature and its main emphasis is on the event that might occur.

According to Render et al (2003:34) there are also two basic rules regarding the mathematics of probability:

---

[6] *Fibonacci (1170 –1240) is an Italian mathematician and also known as Leonardo da Pisa. The Fibonacci sequence 0, 1, 2, 3, 4, 5, 8, 13, 21, … in which each term is the sum of the two preceding terms, occurs in higher mathematics in various connections (The Concise Columbia Encyclopedia, 1989,1991).*

- Probability, *P*, of any event or state of nature occurring is greater than or equal to 0 and less than or equal to 1. A probability of 0 indicates that an event is never expected to occur. A probability of 1 means that an event is always expected to occur;

- The sum of the simple probabilities for all possible outcomes of an activity must equal 1.[7]

A more in-depth discussion on probability concepts and applications follows in Chapter 3 under point 3.2.1.

1.6.7 Threat

According to Ozier (2003a:5) threat is a potentially undesirable event that could result in loss or harm.

The experience of a threat event and its measurable loss or harm is distinct from potential threat events and associated estimates of loss or harm. The aggregation of threat-event experience data provides the basis for estimating expected threat-event loss or harm in the future (Ozier 2003a:6).

1.6.8 Decision theory

Render et al (2003:78) is of the opinion that decision theory is an analytic and systematic way to tackle problems. These problems can help managers in making good decisions, based on logic.

Important in the decision theory is always the following fundamental steps, which will be given more attention to in Chapter 2, paragraph 2.3.1. For the purpose of this discussion the steps can be listed as follows:

---

[7] *Note that when you're dealing with an infinite number of possible events, an event that could conceivably happen might have probability zero. Consider the example of picking a random number between 1 and 10, what is the probability that you'll pick 5.0724? It's zero, but it can happen. (Render et al 2003:35)*

- Define the problem;
- List possible alternatives;
- Identify the possible outcomes or states of nature;
- List the payoff or profit of each combination or alternatives and outcomes;
- Select one of the mathematical decision theory models; and
- Apply the model and make decisions.

1.6.9 Risk Impact[8]

Jenkins (1998:4) describes risk impact as losses as a result of threat activity, which are normally expressed in one or more impact areas. Four areas are commonly used: destruction, denial of service, disclosure and modification. According to Martin and Tate (2002:2) risk impact is the effect the risk will have if it does occur.

Le Roux (2002a: 9) is of the opinion that risk impact is the impact or the consequence of any risk or threat, which has actually happened. According to Ozier (2003a:6) the term impact points to the loss or harm attributable to a threat event, quantitatively derived in monetary terms as Asset Value X Exposure Factor = Impact, or single loss exposure, and qualitatively expressed by a variety of metrics ranging from ordinal ranking to terms such as “minimal”, acceptable”, and “unacceptable”. A more in-depth discussion on the “impact” concept follows in chapter 4.

1.6.10 Private Security

In general it can by said that private security is an independent or proprietary commercial organization whose activities include employee clearance in investigations, maintaining the security of persons or property, performing the

[8] *Risk Impact will form part of a comprehensive discussion in Chapter 4*

functions of detection and investigation of crime and criminals, and apprehension of offenders for reward, fee, or benefit. (Weaver 2003:16).[9]

1.7 SUMMARY OF CHAPTERS

A summary on chapter's 2 to 8 is briefly summarised below.

Chapter 2 – Evolution of private security: theoretical basis

The concentration in this chapter is solely based on the theoretical approach of private security and the risk analysis process. Some concept clarification, structuring and the importance of legislation form a fundamental part of this discussion. Emphasis is also placed on the education of the security manager in quantitative risk analysis as well as the professionalism, which should be practiced at all times within the private security industry. The future of private security in quantitative risk analysis will complete the whole picture.

Chapter 3 – The probability concept within the risk analysis approach

The main thrust of this chapter is to describe the "probability" concept and its application within the analysis process. It will also outline the importance of probability as the first step in the development of the "TIQCAM" model. Lastly, it will form a joined excel formation with the next chapter's concept, which will also be applied to the other chapters. This will smooth the discussion and complete the development of the "TIQCAM" model in chapter 7.

Chapter 4 – Combinational approach of the impact concept

This chapter highlights the impact concept as the second step in the risk analysis approach as well as the combination of "sensitivity" and "severity". The importance that the impact concept cannot function in isolation in developing a quantitative analysis model will form part of the overall discussion.

[9] *A more comprehensive discussion will follow in Chapter 2.*

Chapter 5 – Essentiality of the cost factor in risk measuring

Attention is given to the cost factor as the essential and dynamic concept in the risk analysis process. The development of the “TIQCAM” model involving the cost factor will also lead to the importance of joint relationship with other concepts, such as the degree of correction.

Chapter 6 – Degree of correction as a mitigational concept in the analysis process

Discussion will place the emphasis on the importance of the degree of correction concept in achieving the most accurate outcome of the risk rating in the development of the “TIQCAM” model. The emphasis is also placed on the importance of the combining effect with the cost factor and other concepts in development process.

Chapter 7 – Human factor as a concept in quantitative risk analysis

The discussion in this chapter is totally the initiative of the researcher and places the emphasis on the utmost importance of the human factor, also known as the “CHHP” approach in the development of the “TIQCAM” model. This chapter will also aim to integrate and/or join al the concepts (Chapter 3 –7) together in developing the model. Guidelines for the implementation of the “TIQCAM” model shall conclude this discussion.

Chapter 8 - Findings and recommendations

This is a general summary of the study that was undertaken and supplies an evaluation of the findings relating to the objectives, hypotheses, methodology and empirical data. Certain recommendations are made on the basis of the findings. Future tendencies in respect of further developments of quantitative risk analysis models for private security use are also discussed.

1.8 CONCLUSION

The one major resource required for risk analysis in general, is trained human resources. It is thus necessary for private security managers to be well educated in the use of a workable quantitative risk analysis model. The rationale for this study in this regard is discussed; clarification on key concepts, such as private security and risk analysis aspects are taken in consideration as well as a foresight of the course of this study.

CHAPTER 2

EVOLUTION IN PRIVATE SECURITY: THEORETICAL BASIS

2.1 INTRODUCTION

Padwa (2001:1) states that while the United States economy was booming in the 1990's and (dot) !-com mania was creating the illusions of new wealth, other parts of the low-wage economy were experiencing high growth rates such as the private security industry.

South Africa was also no exception and the growth of the private security industry has its own problems such as training and education. Private security providers also need to increase their professionalism and should start seeing their employees as assets that are a long-term investment.

This researcher intends to sketch a brief historical context of private security in South Africa. This discussion will also share some thoughts on the current status of the industry and finally conclude with the importance of quantitative risk analysis by private security managers.

It is generally believed that a security policy in the future plans of trade and industry is an internationally established practice to overcome the threat against profitability. In South Africa crime remains the single largest threat. The researcher is of the opinion that educating and practicing quantitative risk analysis will not only lower the crime rate but also earn more responsibility that adds value in the customer's eyes and thus place professionalism in the forefront.

The security services industry serves and protects primarily the interest and assets of industry and commerce in order to maintain profitability, economic growth and job creation, as well as to develop welfare and stability among the various communities.

Further, it is the researcher's contention that the private security industry will benefit, in not only educating their managers in business and financial skills, labour relation skills, judicial and commercial knowledge and specialized security practice, but mainly in the quantitative risk analysis process, which forms part of the every day program.

2.2 HISTORICAL CONTEXT OF THE PRIVATE SECURITY INDUSTRY

Contrary to popular belief, private security, particularly as a profession, is not a relatively modern development. A study of history from the beginnings of mankind shows that the protection of life and property is one of the oldest tasks both faced and undertaken by men (Christman 2003a:1).

Because private security as we know it today has developed as the result of a multitude of ideas, concepts, historical events and identifiable individuals and personalities, and because private security has become an essential and necessary ingredient of modern business, industry and society; some knowledge of how it developed is not only interesting but also helpful in understanding this emerging profession and its future.

Although the history of private security can be dated back to the ancient and biblical periods, this discussion will only focus from the 1880's and with the emphasis on the United States and South Africa.

2.2.1 History in Europe and United States

Christman (2003a:1) is of the opinion that the modern–day private security had its beginnings through Sir Robert Peel, Home Secretary of England, who guided a bill through Parliament, entitled "An Act for improving the police in and near the Metropolis". World War II was the real source and stimulus of the modern and complex private security industry today. Private security actually came off the ground in the mid 1880's. According to Christman

(2003a:2) Allen Pinkerton, a former policemen, was the first to form a private agency, specialising in providing security services for railroads and industrial organisations. The Pinkerton, Brinks and Burns companies all continue in business today.

Beginning in the second half of the 20th century, private security (whether proprietary or contractual) has played an increasingly larger role in crime control and prevention, so that as of 1985 the resources of money (over 20 billion dollars annually) and personnel (over 700,000) exceed that of public law enforcement. The most recent trend is the "privatisation" of functions such as running jails and prisons, which were previously the jobs of government exclusively (Christman 2003a:5).

Private security is big business in all free-world countries and ranges from the single owner/operator private detective agency or security consultant through national contract security guard companies and investigative agencies, to multi-national security firms and alarm companies. The thousands of proprietary security personnel, working only for a single employer and in his interests only, must also be included (Christman 2003a:5).

According to Christman (2003a:5) the industry, because of its size, has begun to attract the attention of legislatures and of the courts, and in those instances where self-restraint and legal and ethical considerations are neglected, the legislatures and courts are establishing the standards under which we the private security Industry are required to operate. In other cases, the courts are also punishing, through monetary awards to injured parties, those private security practitioners who "go too far" and offend public sensibilities.

The Industry is also growing in sophistication and professionalism. It is attracting personnel and leaders who would be a credit to any profession. With both continued growth and professionalism, which seems assured, the future of private security and that of those in the profession, seems bright (Christman 2003a:6).

2.2.2 History in South Africa

In South Africa the private security has a number of unique features because of the political context in which the industry developed. In Europe and the US, the security Industry's expansion in the 1970's and early 1980's occurred without any real input or assistance from the state. This was not the case in South Africa (Irish : 1999:1).

In the late 1970's and throughout the 1980's, the former South African Police (SAP) withdrew from many normal policing duties to concentrate on maintaining political control. The Government encouraged the private security Industry to fill the gap left by the police's shift in priorities, which led to a close relationship between private and public policing, but with different goals. The Government also assisted the Industry by providing mechanisms with which the Industry could link up formally with the State security apparatus. In 1991, at a Security Association of South Africa (SASA) conference, Lieutenant General Basie Smit hinted at the establishment of a joint working committee to produce a blueprint on co-operation between the SAP and the private security Industry. In 1992, the then Commissioner of Police, General Johan van der Merwe, considered the creation of a permanent secretariat consisting of SAP and private security industry representatives (Irish 1999: 1).

Irish (1999: 1) also indicates that at a formal level, the state used private security companies to guard strategic installations. In 1980, The National Key Points Act was passed. Act No.102 of 1980, granted greater powers to the private security guards who were tasked with guarding strategic installations, including full powers of arrest, and search and seizure.

The question whether the Government at the time and those working in the private security industry had similar interests has been raised on several occasions. Many security companies have strongly refuted any allegations of mutual interest. However, according to members of the Security Officer's

Board, the government might have channelled funds into certain private security companies and used them as front companies (Irish 1999: 1).

Because of South Africa's past involvement in military operations in other African states, and the immigration to South Africa of people who fought in the bush wars in the then Rhodesia and other African states, a large number of people with experience in counterinsurgency and low intensity conflict operations live in South Africa. Not surprisingly, many owners and managers of private security companies have military, intelligence and police backgrounds. One security company manager said initially it was his company's policy only to recruit people who had been members of the SAP. In the 1970's, the policy was extended to include army and correctional services personnel (Irish 1999: 1).

According to Irish (1999:1), many companies still regard the recruitment of personnel with a previous security background as desirable. The involvement of former military and police personnel has had a marked impact on the profile, structure and training and even uniforms of private security companies in South Africa. There is a large group of people with combat experience who fought both for and against apartheid who find a natural home in the private security industry, both in their capacity as employers and employees. Some of these individuals, who have been forced to take early retirement because of their past involvement in apartheid-sponsored violence, are qualified for little else than narrowly defined security work.

Another common area is that of investigation of crime. It was not uncommon to find security guards involved in unlawful methods of interrogation. There have been a number of reports of security personnel being actively involved in the interrogation and torture of suspected bank robbers or of internal investigation units interrogating their own guards who have been suspected of involvement in inside jobs (Irish 1999:1).

2.2.2.1 Private security after 1994

After the first democratic elections in 1994, the levels of reporting crime increased dramatically and the true extent of violent crime as distinct from political crime began to emerge.

May (1996:130) is of the opinion that the state of emergency from 1985 to 1990 probably suppressed crime levels, as well as the reporting and recording of those crimes that did occur. Political liberalization in the early 1990's witnessed an apparent crime explosion as social controls were loosened and police were released from duties of suppressing political violence. During this period the crimes committed, particularly property crimes, were accompanied by excessive violence.

According to Schönteich (2002:11) over a ten-year period, between 1988 and 1997, the number of reported murders and rapes increased two and a half times and reported robberies almost three times. Serious crimes against property also rose considerably over that period. Dempster (2002:1) is of opinion that crime increases get to the situation where no matter how hard you work, and no matter what you do, you can never stop crime.

Consequently, many companies and individuals who could afford to engage the services of private security companies, particularly armed response, did so thereby continuing the trend that existed before 1994. Although private security companies seem able to respond faster to calls for assistance, they are still seen by most affluent South Africans as a "grudge buy", a purchase they would rather not have to make (Dempster 2002:3).

The other main concern is that of the poorer companies that cannot afford the services of private security companies. This entrenches the

disparities between the rich and the poor, which actually implies that policing in South Africa is spread unevenly such as in the black communities. This latter also contributes to the growth of the private security industry.

The private security industry seeks to protect the interests of its paying customers, while the police act in public interest. It can thus be said that security companies are focused more on the prevention of loss than the detection of offenders. The exercise of discretion by private security personnel will be far more influenced by their perceptions of the interests of their immediate employer than on any generalized conception of the public interest. Offenders will only be handed over to the police if this is in the perceived interest of the customer.

It is also necessary to point out that the private security personnel don't have the same legal powers as Police members. Private security officers only have the same rights as citizens.

Private security officers do however have discretion once they are in the private property of their customers.

2.3 DEFINITION OF CONCEPTS

As stated in Chapter 1 under point 1.6, it is now necessary to elaborate on the following concepts.

2.3.1 Private security

Fischer and Green (1992:74) indicate that private security includes those self-employed individuals and privately funded business entities and organizations providing security-related services to specific clientele for a fee, for the individual or entity that retains or employs them, or for themselves, in order to protect their persons, private property, or interests from varied hazards.

The South African Police Service is actually of the opinion that with the upliftment of deprived communities and the role public and private institutions/organizations have to play in the Reconstruction and Development Programme, the following fundamental question needs to be answered: Must poor people be dependent on the public police for protection while those who can afford it, buy their own (professional) security? (Van Vuuren 1998:13).

According to Bosch (1999:4) private security refers to those efforts by individuals and organizations to protect their assets from loss, harm or reduction in value, due to criminal actions.

The researcher is of opinion that private security in South Africa is plain and simple. It can be seen as that of a non-government company, which is only compelled to render a service to their clients who can afford their services.

Private security is also called contract security. In South Africa the business society is more familiar with the term contract security. For the purpose of this study the focus will mostly be on the term “private security”.

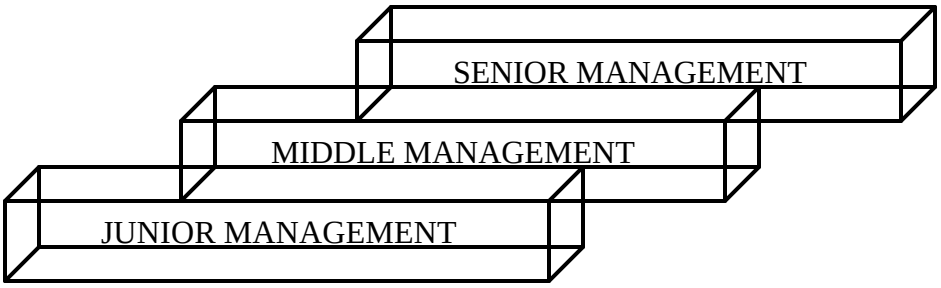
2.3.2 Private security manager

A private security manager is a manager employed by a private security organization in rendering a security service to their clients. The security manager must be registered according to the Private Security Industry Regulatory Act, Act 56 of 2001 and must be an “A”-grade, which means that the focus is on the total spectrum of security management.

The term security manager also indicates that management is a fundamental part of the whole security process. According to Marx, Van Rooyen, Bosch and Reynders (1998:352) management is a rational process, which focuses on resources such as planning, organizing, leadership, coordination and control to reach for goals.

According to Le Roux (2002b:4) management can also be categorized in a three- step pathway as shown in figure 2.1 below.

Figure 2.1: Three-step career path of management



Source: Own compilation

For the purpose of developing a quantitative risk analyses model for the private security manager and for this study as a whole, the term security manager will include all three the career paths of management.

2.3.3 Physical security

The fact that this study concerns the physical security risk aspects, it is also necessary to give a brief definition on physical security. According to Rogers (1997:25) physical security is aimed at the implementation of physical barriers in order that risks may be managed. These risks include a wide variety of crimes such as robbery, fraud, theft, housebreaking and vehicle theft.

One of the main basic principles of any physical programme or system according to Van der Westhuizen (1989:5), is the analysis and decision making to prevent and control crime-related losses.

It is also of the utmost importance for the security manager to know and understand risk, the term risk analysis and quantitative risk analysis. A brief discussion of the latter terms follows.

2.3.4 What is risk?

Risk is associated with virtually every activity one can think of, but for the purpose of this discussion, it will be limited to the uncertainty of financial loss. According to Broder (2000:1) it can also indicate damage or any other undesirable event. Kastrup (2000:2) perception is that risk can also be defined as the probability that certain damage will occur. Risk analysis should also examine the vulnerability of an object, which can be defined by two questions: First, how easy is it to cause damage to the object; and second, how much time and efforts are required to revert to the "status quo ante", that is, the state before the damage occurred (Kastrup 2000:2). Most people desire low risk, which would translate to a high probability of success, profit, or some form of gain.

Almost any change, good or bad, poses some risk. The analysis will usually reveal numerous potential risk areas: overtime costs, inventory shortages, future sales, geological survey results, personnel fluctuations, unpredictable demand, changing labour costs, etc. The division of risk can be limited to three common categories according to Broder, (2000:1):

- Personal (having to do with people's assets)
- Property (having to do with material assets)
- Liability (having to do with legalities that could affect both of the above, such as errors and omissions, wrongful discharge, workplace violence, and sexual harassment, to name a few of the most current legal issues that plague the business community).

Le Roux (2002a: 1) indicates that risk also takes many forms. It is therefore necessary to use systematic processes and tools to understand and prioritise risks, especially those with catastrophic consequences. Traditionally, we have measured risk in the following way:

Risk = Frequency (F) x Consequence (C)

In this equation;

Frequency (F) = Initiating event frequency x probability of all safeguards fail

On the other hand, in security risk management the frequency element of the above equation is separated into two parts as:

Risk = [Threat (T) x Vulnerability (V)] x Consequence (C)

According to the above equation;

- Threat is the measure of the likelihood that a specific type of attack will be initiated against a specific target;
- Vulnerability is the measure of the likelihood that various types of safeguards against a scenario will fail;
- Consequence is the magnitude of the negative effects if the attack is successful.

So, it can be noted that risk can be measured in the same way, but with slightly different terminology.

2.3.5 Risk analysis terminology

There may be some terminology and definition differences related to risk analysis, risk assessment and business impact analysis. Although several definitions are possible and can overlap, the following terminology and definition of Wold and Shriver (1997:1-2) can be considered:

- A risk analysis involves identifying the most probable threats to an organization and analysing the related vulnerabilities of the organization to these threats;
- A risk assessment involves evaluating existing physical and environmental security and controls, and assessing their adequacy relative to the potential threats of the organization;
- A business impact analysis involves identifying the critical business functions within the organization and determining the impact of not

performing the business function beyond the maximum acceptable outage. Types of criteria that can be used to evaluate the impact include: customer service, internal operations, legal/statutory and financial issues.

Jenkins (1998:4) is of the opinion that in order to discuss security risk analysis concepts, a baseline must first be established of related terms and how they are used to analyse risk. The following terms are applicable:

- Asset – Anything with value and in need of protection;
- Threat – An action or potential action with the propensity to cause damage;
- Vulnerability – A condition of weakness. If there were no vulnerabilities, there would be no concern for threat activity;
- Countermeasure – Any device or action with the ability to reduce vulnerability;
- Expected loss – The anticipated negative impact to assets due to threat manifestation;
- Impact – Losses as a result of threat activity are normally expressed in one or more impact areas. Four areas are commonly used, namely destruction, denial of service, disclosure and modification.

Jenkins (1998:4) furthermore explains how related terms work together. According to him a security risk analysis is an examination of the interrelationship between assets, threats, vulnerabilities and countermeasures to determine the current level of risk. The level of risk that remains after consideration of all in-place countermeasures, vulnerability levels, and related threats is called residual risk.

Any given threat in the population of threats is poised to take advantage of system vulnerabilities; countermeasures reduce the level of vulnerability, the asset is what needs to be protected, and the impacts are the result of threat activity through residual risk.

According to Broder (2000:2) risk analysis is a management tool which main function is the identification of assets that need protection. The probability of risk occurrences and the impact or effect is then to be considered for implementing the right countermeasures. Although Broder's view is the same as the authors Jenkins (1998:4) and Wold and Shriver (1997:1-2) regarding the related terms used in risk analysis, he rather places the emphasis on the term "estimating" than "analysis". Broder (2000:2) argues that risk analysis will never be an exact science and that the term "estimating" is fairly easy to use to estimate the probability of occurrences or events.

Taking Broder's argument into account, the researcher is of the opinion that the term "estimating" is historical in the sense that in 431 B.C, the term was used in an excerpt from Pericle, an Athenian general's speech (See point 2.3.1.2).

The terminology "risk analysis", "risk assessment", "risk evaluation" and "risk estimating" are sometimes also considered to be the same conception. The question can thus be asked: What are the differences between the abovementioned terminologies or is there any difference at all? Addison (2002:2) indicates that risk analysis is also known as risk assessment, which focuses on the process of identifying the hazards and their causes, determining the consequences of the hazards, and calculating the probability of their occurrences. The perception that calculation, which forms part of the risk assessment and/or risk analysis process, can also interoperate as estimating of an occurrence.

Berryman (2002:2) is of the opinion that the focus must be on risk assessment rather than risk analysis. To him, risk assessment means the gathering of information, which means that the data itself must be estimated to get to the cost factor.

Addison (2002:3) is of the opinion that there is a definite difference between the terms "assessment" and "analysis". Assessment focuses on the financial

and business aspects while analysis is associated with the personal insights of the company's personnel. Schirick (2000:1) is of a different opinion regarding the perception of Addison (2002:3). To him, risk analysis and evaluation has one meaning, which also focused on the process of identification and estimating the costs.

According to Render et al (2003:2) analysis and specifically quantitative analysis is a scientific approach to managerial decision-making. Whim, emotions, and guesswork are not part of the quantitative approach. This approach starts with data. Like raw material for a factory, these data are manipulated or processed into information that is valuable to managers in making decisions.

Whatever the different views may be, the researcher is of the opinion that the foresaid terms are so closely associated with each other in the overall process that the main objective must be to link all the information gathered to assist businesses to manage their risks.

Within the scientific framework of risk analysis, risk communication is an important management tool for making critical decisions, and in some cases meeting regulatory requirements. According to Reksnes (2003:1) communication in the recent years has been acknowledged as playing an important part, often decisive as regards the outcome or effect of risk assessment and risk management on opinions or behaviours. For the purpose of this discussion the following definition of risk communication by Reksnes (2003:1) can be used as - "Access to information and participation in the process of risk analysis".

2.3.6 Quantitative risk analysis

According to Render et al (2003:2) quantitative analysis is the scientific approach to managerial decision-making. Whim, emotions and guesswork are not part of the quantitative analysis approach. The approach starts with data.

Like theft or fraud in a company, this data is manipulated or processed into information that is valuable for decision-making purposes. Computers are instrumental in the increased use of quantitative analysis (see 2.10). According to Berryman (2002:6) the quantitative approach is not widely used because it involves calculating numerically the probability when an event will occur, then assigning an amount to the impact of the occurrence, which will not always reflect a true version of both the probabilities and impact.

The other approach, and the most widely used form of calculating risk, is the qualitative approachability. Berryman (2002:6) is of the opinion that this involves subjectively rating the probability and the impact. What needs to be considered is that for each vulnerability rate, the probability may occur. It must be indicated as high, medium or low. Then independently rate the cost this may have on the organization as high, medium or low. To do this, Berryman (2002:6) suggests that data input from the business community plays a vital role in rating the cost, because in most environments, they are considered the owners of the data. So obviously, if a particular vulnerability has a high probability of occurring and a high dollar impact if it were to occur, the risk would be considered high.

According to Le Roux (2002a: 2) both quantitative and qualitative factors should also be considered. The weather, legislation and social economical aspects may all be factors that are difficult to quantify. Because of the importance of qualitative factors, the role of quantitative analysis in the decision making process can vary. When there is a lack of qualitative factors and when the problem, model and input data remain the same, the results of quantitative factors can automate the decision making process. For example, some companies use quantitative inventory models to determine automatically when to order additional new material/equipment. In most cases, however, quantitative analysis will be an aid to the decision-making process (Render et al 2003:2).

For the purpose of this study, the researcher is of the opinion that the quantitative approach is more fundamental in the exact prioritising of risks if all quantitative factors are taken into consideration, and not only the probability and impact of risk as indicated by Berryman (2002:6) The different concepts shall be dealt with in Chapter's 3 to 7.

2.4 BASIC OVERVIEW IN UNDERSTANDING QUANTITATIVE RISK ANALYSIS BY PRIVATE SECURITY

It is important that the security manager be acquainted with the quantitative risk analysis approach and also understands that the term "quantitative" mainly involves mathematics. The researcher's perception is that this understanding should be the basics when educating the security manager in quantitative risk analysis as discussed below.

2.4.1 Mathematics, analysis and management in history

Historical information regarding mathematics, analysis and management gained from the Concise Columbia Encyclopedia (Levey & Greenhall 1985:1089) is as follows:

2.4.1.1 Socrates role in mathematics

It can be said that Socrates (469-399 BC), Greek philosopher, Athens, is regarded as one of the wisest men of all time in mathematics. It is not known who his teachers were, but he seems to have been acquainted with the doctrines of Parmenides, Heraclitus and Anaxagoras[10]. Socrates himself left no writings, and most of our knowledge about mathematics comes from the dialogues of his most

[10] *Parmenides (515 BC), Pre-Socratic Greek philosopher. Major contribution to the method of reasoned proof assertions.*
Heraclitus (535 –475BC), Greek philosopher. He taught that there is no permanent reality except the reality of change, a position illustrated by his famous maxim "You cannot step twice in the same river."

famous pupil, Plato[11] and from the memoirs of Xenophon[12]. Mathematics is very broadly divided into foundations, algebra, analysis and geometry. From his interest in the mathematics, it can thus be said that the quantitative theory arose from where it is used today as a modern physical theory in the quantitative analysis approach (Levy & Greenhall 1985:1089).

2.4.1.2 Origination of mathematics and analysis

The earliest records according to Levy and Greenhall (1985:1089), indicate that mathematics arose in response to the practical needs of agriculture, business, and industry in the 3rd and 2nd millennia BC in Egypt and Mesopotamia, and possibly India and China. Mathematical analysis shows that analysis was done on a basis of individual knowledge with little or none scientific techniques during the period of imperialist colonization in the 16^{th}-19^{th} centuries on archaeology. Scientific techniques and systematic methodologies became increasingly useful towards the end of the 19^{th} century when archaeology is driven as an academic study. The main risks that were faced by archaeologists during the rescue of physical remains are the excavation of sites at risk from deep ploughing, quarrying and road laying.

According to Render et al (2003:3) mathematical analysis (also called quantitative analysis) has been in existence since the beginning of recorded history, but it was Frederick W. Taylor who in the early 1900's pioneered the principles of the scientific approach to management.

Anaxagoras (500-428BC), Greek philosopher, thought to have been the teacher of Socrates. He held that an all-pervading onus (world-mind) ordered the physical world by combining particles from the undifferentiated mass of the universe.

[11] *Plato (427-347BC), Greek philosopher and famous pupil and friend of Socrates. His extant work is in the form of epistles and dialogues divided according to the probable order of composition.*

[12] *Xenophon (430-355), Greek historian. A well-to-do young disciple of Socrates. His most famous work, the Anabasis, was written in exile in Sparta.*

Stamatelatos (2000:4) points out that historically, risk assessment can be traced back in 431 B.C. The following is an excerpt from a speech of Pericle, an Athenian general, to his troops before a battle in the war between Athens and Sparta:

" We the Athenians in our own persons, take our decisions on policy and submit them to proper discussion. The worst thing is to rush into action before the consequences have been properly debated. And this is another point where we differ from other people. We are capable at the same time of ***TAKING RISKS AND ESTIMATING THEM BEFOREHAND.*** *Others are brave out of ignorance, and when they stop to think, they begin to fear. But the man who can most truly be accounted brave is he who best knows the meaning of what is sweet in life, and what is terrible, and he then goes out undeterred to meet what is to come".*

Thus can it be said that the past paved the way for risk analysis in all sectors of the community today. Risk analysis is now regarded as mandatory in many quarters, for example by the Government for all its new IT projects. Also in the private sector, particularly public listed companies and those who are seeking a public listing, need to comply with the Turnbull (UK) Report on Corporate Governance requirements, which prescribes undertaking an analysis of business risks (Shaw 2002:1). This is also applicable to South African companies concerning corporate governance as laid out in the King report (King: 1994:5).

During World War II, many new scientific and quantitative techniques were developed to assist the military. These new developments were so successful that after World War II many companies started using similar techniques in managerial decision making and planning. Today, many organizations employ a staff of

operations research or management science personnel or consultants to apply the principles of scientific management to problems and opportunities (Render et al 2003:3).

Many of the techniques and principles of scientific management discussed in this study were first developed by Taylor (Render et al 2003:3).

2.4.1.3 The quantitative risk analysis approach

Many authors have different views regarding the quantitative analysis approach. Martin and Tate (2002:1) use the Step-by-Step approach in analysing risk. Quantification is the main step by which a team determines the risk ratings for each risk. The second step is the evaluation approach. The approach by Martin and Tate (2002:2) is mainly to rate the probability and the impact of each risk.

Davis (2002:01) is of the opinion that quantitative approach consists only of hazard identification and impact analysis. This approach is not adequate enough to train individuals in the total quantification approach. The probability, cost of risk and degree of correction are not taken into consideration with their quantitative approach. As in the case of Martin and Tate (2002:1), no exact quantification can be done if the whole of the quantification approach is not adhered to. This means that factors such as developing a model, and testing the model before implementing the results should be taken into account.

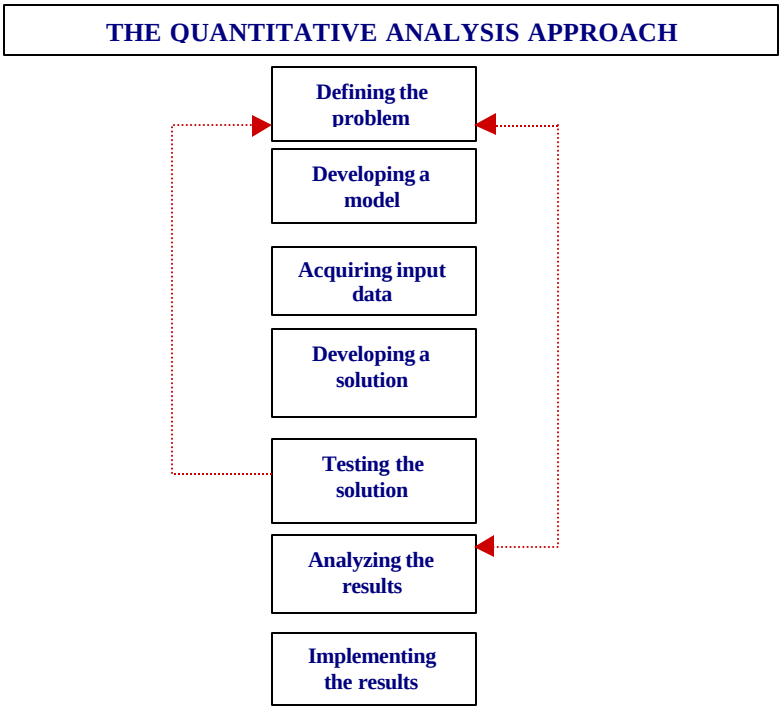
According to Blackburn (2002:5) it is important that by identifying, recording and monitoring potential risk across the organization permits sophisticated analysis techniques to be used. Quantifying risks allow the manager to perform analysis in all parts of the organization. However, the researcher is once again of the opinion that this is not the right way of approaching the quantification of

risks. This approach is not really a quantitative approach but rather a process. If one looks at the Risk Management process it indicates that risks must first be identified, then evaluated and then risk controls and or actions can be applied.

It is the researcher's perception that the said approaches will make it really difficult for the security manager to cope. It is the aim of the researcher to provide a quantitative risk analysis model (see chapter 7), which is easy to use and thus provide the security manager with a tool that is reliable and as far as possible, trustworthy.

Render et al (2003:3) is of the opinion that as with the normal quantitative analysis approach, the quantitative risk analysis approach will also consist of defining the problem, developing a model, acquiring input data, developing a solution, testing the solution, analysing the results and implementing the results (see Figure 2.1).

Figure 2.1: The quantitative analysis approach



Source: Render, Stair and Hanna (2003:3)

2.4.1.3.1 Defining the problem

According to Render et al (2003:3) the first step in the quantitative approach is to develop a clear concise statement of the problem. The statement will give direction and meaning to the following steps. Problem focusing must always be on selecting those problems whose solutions will result in the greatest increase in profits or reduction in costs to the company.

2.4.1.3.2 Developing a model

Once the problem is selected to be analysed, the next step according to Render et al (2003:3) is to develop a model. A model is a representation (usually numerical or statistical) of a situation. There are many types of models. Architects sometimes make a physical model of a building that they will construct. Engineers develop scale models of chemical plants. A schematic model is a picture, drawing or chart of reality. What sets quantitative analysis apart from other techniques is that the models used are mathematical. A more comprehensive discussion on this subject will be dealt with in Chapter 7.

2.4.1.3.2 Acquiring input data

Once a model is developed, data must be obtained to be used in the model. According to Render et al (2003:4) obtaining data for the model is essential and must be a representation of the reality. Improper data will result in misleading results.

There are a number of sources that can be used in collecting data. In some cases, company reports and documentation can be used. Interviews with employees can also reveal with a great degree of accuracy the amount of time in producing a product, etc. Insurance companies can also be of great help in collecting data.

2.4.1.3.3 Developing a solution

The input data and the model not only determine the accuracy of the solution but also involve manipulating the model to arrive at the best (optimal) solution to the problem. Render et al (2003:5) states that if the input data are accurate to only two significant digits, then the results can be accurate to only two significant digits. For example, the results of dividing 2.6 by 1.4 should be 1.9, not 1.857142857.

It is researcher's opinion that instead of developing and reporting one solution, the quantitative analysts should at least produce more than one solution. This allows more discretion in the decision-making process and also leaves the door open for wider use (e.g. planning and decision making which is levelled on the same functional line).

2.4.1.3.4 Testing the solution

Assumptions of the model and the solution must always be carefully tested. According to Render et al (2003:5) there are several ways to test input data. One method of testing the data is to collect additional data from a different source. If the original data were collected using interviews, perhaps some additional data can be collected by direct measurement or sampling. These additional data

can then be compared with the original data, and statistical tests can be employed to determine whether there are differences between the original data and the additional data.

2.4.1.3.5 Analysing the results

Render et al (2003:5) not only place the emphasis on analysing the results, but also place a great degree of importance on sensitivity analysis. Sensitivity analysis determines how the solutions will change with a different model or input data. Because input data may not always be accurate or model assumptions may not be completely appropriate, sensitivity analysis can become an important part of the quantitative analysis approach.

2.4.1.3.6 Implementing the results

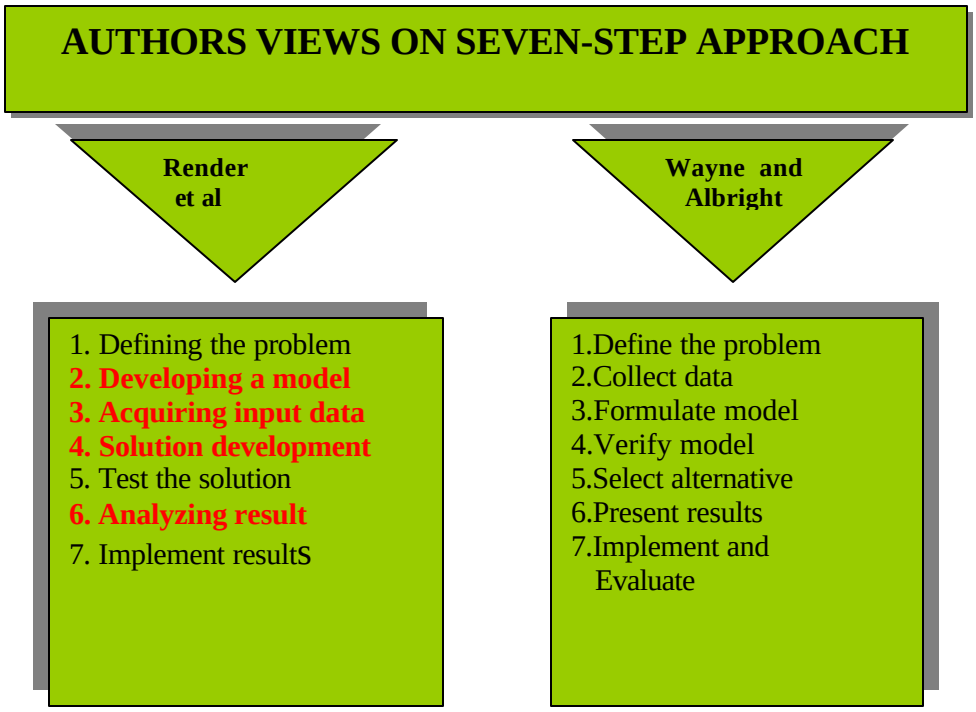
The final step is to implement the results. After the solution has been implemented, it should be closely monitored. According to Render et al (2003:3) there may be numerous changes that call for modification of the original solution. A changing economy, fluctuating demand, and model enhancements requested by managers and decision makers are only a few examples of changes that might require the analysis to be modified.

Wayne and Albright (1997:8-9) also support the seven-step process but in a different approach. They fully agree on the first step in defining the problem. The second step should be the collection of data and then the developing of the model, which is not the case with Render et al

(2003:7) steps. Acquiring input of data forms part of the latter author's steps.

Figure 2.2 illustrates the comparison of both Render et al (2003:3-6) and Wayne and Albright (1997:8-9) seven step modelling process.

Figure 2.2: Comparison of a seven-step modelling process



Source: Own compilation

Although the researcher agrees that both the authors' perceptions on the seven-step modelling process is just a process followed in making the end product work, he would rather support the approach by Wayne and Albright (1997:8-9) because no development of a model can take place unless the input data is collected beforehand.

Although there is not a big difference in both the Render et al (2003:3-6) and Wayne and Albright (1997:8-9) processes, it

remains their prerogative to approach their models in their own way.

The application for this study will be based on Wayne and Albright (1997:8-9) process regarding the quantitative risk analysis model for the private security managers.

Step 1: Define the problem

Problem is that no quantitative risk analysis model exists for the private security managers to analize physical and quantifiable risks, for example robbery and fraud.

Step 2: Necessary data is collected (informal interviews as discussed in Chapter 1 under points 1.5.3.1 and 1.5.3.3.

Step 3: In Chapter 5 the focus will be solely be on the development of a quantitative risk analysis model for security managers, which will deal with probabilities, impact etc., regarding the risk situations.

Step 4: The model will then be verified for its accuracy. If not accurate, alternatives will be selected as per step 5.

Step 5: Selection of alternatives means that the developed model be tested against other existing models, if they exist. Otherwise this model will then be called an easy-to-use model for security managers.

Step 6: Presentation of the model is the involvement of security managers in the use thereof. This is called the testing period to test the workability of the developed model.

Step 7: The implementation of a quantitative risk analysis will be a contribution for the security industry. Regular evaluation of the model will take place in order to secure its accuracy.

2.4.2 Possible problems in the quantitative analysis approach

Regarding the above quantitative analysis approach by Wayne and Albright (1997:8-9), it is the researcher's perception that this is a more acceptable approach but there are the following possible problems:

Defining the problem, managers are not always proactive in handling problems. They sometimes wait for a problem to arise and then attack the problem until it is solved. Once it is solved, they then sit back and relax until the next problem arises.

Conflicting viewpoints in defining the problem also exists. Financial managers may have a different viewpoint and approach regarding defining the problem. They usually feel that the inventory is too high, as inventory represents cash not available for other investments. Sales managers, on the other hand, often feel that the inventory is too low, as high levels of inventory may be needed to fill an unexpected order. For the security manager, physical aspects (theft, fraud, etc.) will always be rated as high on both financial and the physical sides, unless proper control measures are implemented.

The main concern in developing a model is the understanding of the model. Managers simply will not use the results of any model they do not understand. One approach is to start of with a simple model and make sure that it is completely understood. Such a simple and easy to use model is demonstrated in tables 2.2, 2.3 and 2.4.

Collecting data plays a major role in the whole of the quantitative analysis approach and the emphasis must be placed on validity. A lack of good, clean data must always be distilled and manipulated before used in a model. It often

happens that data is of a subjective nature and will not always reflect the true version thereof. It is a known fact that two persons will have their own views regarding a subject and therefore data, which is represented by them, will have a subjective connotation.

The development of a solution is normally based on the understanding philosophy. Understanding of the mathematics can cause problems for managers that are not using it in their day-to-day activities even though the models are complex and powerful. The second problem is that quantitative models usually give just one answer to a problem. Render et al (2003: 15) go further by saying that managers would like to have a range of options and not be put in a take-it-or-leave-it position.

When testing the solution managers are always asked how good the solution looks to them. This creates problems in the sense that managers in different disciplines don't always see eye to eye. For one the solution is acceptable and for the other not. Mainly the big rejection is when the model is too complex and tends to give solutions that are not intuitively obvious.

The biggest problem in analysing the results is when the results indicate large changes in the organization's policy; the quantitative analysis model can be rejected.

In the researcher's experience over the years, there is a lack of management support and user involvement in the successful implementation of systems. The implementation of a quantitative analysis model can thus also cause problems if top management doesn't force their authority down to junior and senior management in using quantitative analyses.

2.4.3 Mathematical tools in the quantitative approach

It is generally known that computers play a fundamental role in mathematical calculations. This makes the steps such as developing a solution, testing the solution and analyzing the results much easier (See figure 2.1). The following

discussion on the computer is taken from "The Concise Columbia Encyclopedia"(Levey & Greenhall 1985:998).

2.4.3.1 History

Although the development of digital computers is rooted in the abacus[13] and early mechanical calculation devices, Charles Babbage[14] is credited with the design of the first modern computer. The first fully automatic calculator was the Mark I, or automatic sequence controlled calculator, began in 1939 at Harvard by Howard Aiken, while the first all-purpose electronic digital computer, ENIAC (Electronic Numerical Integrator And Calculator), which used thousands of vacuum tubes, was completed in 1946 at the University of Pennsylvania.

UNIVAC (Universal Automatic Computer) became (1951) the first computer to handle both numerics an alphabetic data with equal facility. First-generation computers were supplanted by the transistorised computers of the late 1950's and early 1960's, second-generation machines that could perform a million operations per second. The third-generation integrated-circuit machines of the mid-1960 and 1970's, in turn, replaced them. The 1980's were characterized by the development of the microprocessor and the evolution of increasingly smaller but powerful mini computers, and personal computers.

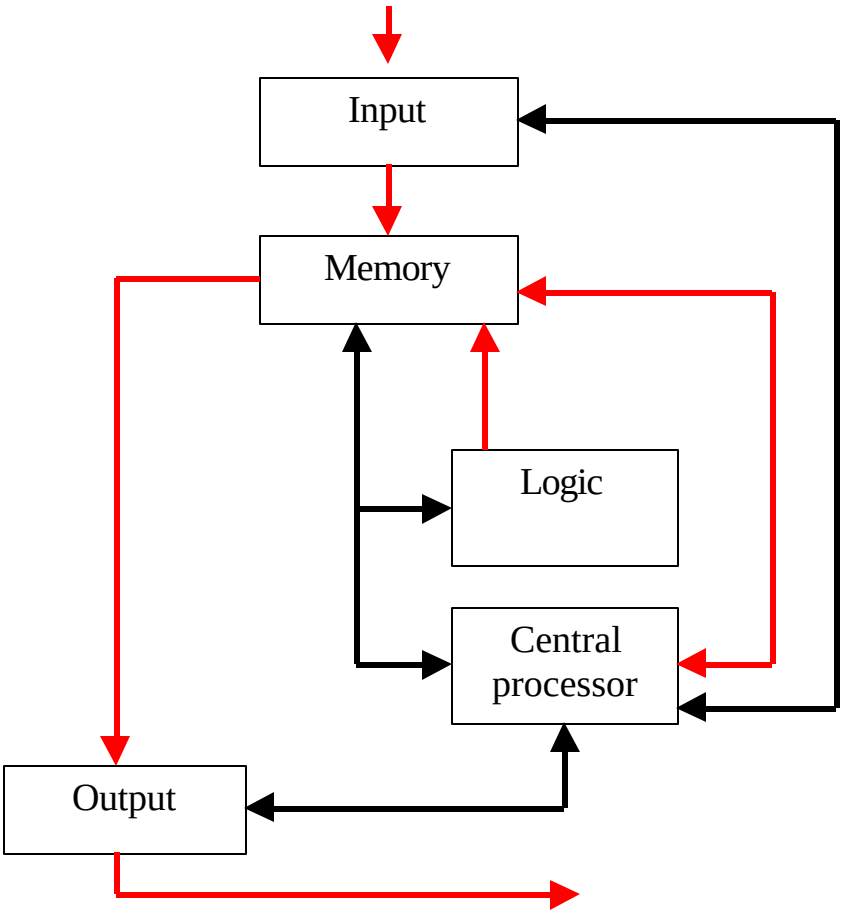
2.4.3.2 Computer

A computer is a device capable of performing a series of arithmetic or logical operations. A computer is distinguished from a calculating machine, such as an abacus or electronic calculator, by being able to

[13] *Abacus, an ancient computing device using movable beads strung on a number of parallel wires within a frame. Each wire represents a decimal place: ones, tens, hundreds, and so on. The beads are grouped to form numbers and shifted in specified patterns to add, subtract, multiply or divide.*

store a computer program (so that it can repeat its operations and make logical decisions) and to store and retrieve data without human intervention. A schematic illustration of a computer system as per Figure 2.3.

Figure 2.3: Schematic illustration of a computer system :red lines indicate data flow; black lines indicates control signals.



Source: Levey and Greenhall (1985:998)

Computers are classed as analog or digital. An analog computer operates on continuously varying data. A digital computer performs operations on discrete data. An analog computer represents data as

---

[14] *Charles Babbage, 1792 –1871, English mathematician and famous for his attempts to develop a mechanical computational aid he called the "analytical engine". Although it was never constructed and was decimal rather than binary in conception, it clearly anticipated the modern digital computer.*

physical quantities and operates on the data by manipulating the quantities. In a complex analog computer, continuously varying data are converted into varying electrical quantities and the relationship of the data is determined by establishing an equivalent relationship, or analog, among the electrical quantities. Analog computers have been nearly completely replaced by more effective digital computers. Within a digital computer, data are expressed in binary notation, i.e., by a series of “on-off” conditions that represent the digits “1” and “0”. A series of eight consecutive binary digits, or bits, is called a byte and follows 256 “on-off” combinations. Each byte can thus represent one of up to 256 alphanumeric characters. Arithmetic comparative operations can be performed on data represented in this way and the result stored for later use. Digital computers are used for reservation systems, scientific, investigation, data processing applications, and electronic games.

2.4.3.3 Personal computer

Personal computer (PC), a small but powerful computer primarily used in an office or home without the need to be connected to a larger computer. PC’s evolved after the development of the microprocessor made possible by the hobby-computer movement of the late 1970’s, when some computers were built from components or kits. In the early 1980’s the first low-cast, fully assembled units were mass-marketed. The typical configuration consists of a video display, keyboard, logic unit, and storage device and, frequently, modem. Some current PC’s have more computing power than the large mainframe computers of the 1950’s and early 1960’s.

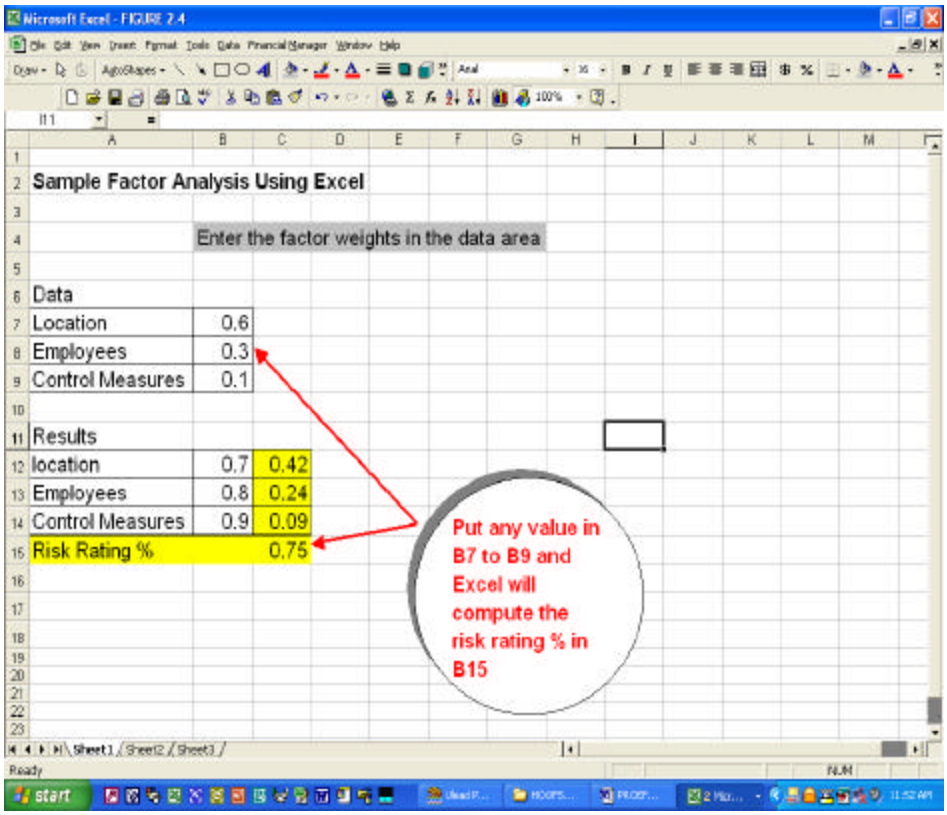
2.4.3.4 Excel spreadsheet tool

One of the main mathematical tools used on computers is the spreadsheet model. Many add-in programs exist to make Excel,

which is already a wonderful tool for modelling, even more powerful in solving quantitative analysis problems. For the purpose of this study, the focus will be on excelling spreadsheet modelling.

To illustrate the Excel spreadsheet tool, a risk factor analysis is used. The example in table 2.2 (only involves branch 1) focused on the input data and the results, in an attempt to supply the reader with more insight in the use and developing of a quantitative risk analysis model (see figure 2.4).

Figure 2.4: Example factor risk analysis by using Excel



Source: Adapted format from Render et al (2003:11)

Hayes (2003:3) openly admits his addiction to Microsoft Excel. After working with the tool for over ten years he decided to create a website that offers free material and solutions for Excel spreadsheet users. Researcher agrees with the latter author that spreadsheet modelling is the only tool that is easy understandable and workable. The aim of this

study will then be to develop a quantitative risk analysis model for private security managers making use of a spreadsheet tool.

2.4.4 Qualitative versus quantitative approaches

According to Ozier (2003b:3) qualitative approaches are characterized by subjective risk measures such as ordinal ranking (low risk or .3-value, medium risk or value, and high risk or value) in a risk-to-value matrix. The qualitative methods emerged in part from a persistent belief that it was simply too difficult to get the real numbers. Also, qualitative approaches appealed to management, which was looking for the "least-effort" way to prove they had assessed their risks. After all, little attention has been paid to the results of risk analysis and assessment until recently (Ozier 2003b:3).

In the researcher's experience, and he agrees with Ozier (2003b: 3), qualitative approaches, however otherwise encouraged, provide little basis for illustrating the scale of risk in monetary terms or for making informed risk-management decisions. The metrics of qualitative risk analysis do not reflect independently objective values such as the monetary value of an asset, the annualised rate of occurrence (frequency), the single loss exposure (impact), or the probability of loss. Although these qualitative metrics can be useful to establish to management that a problem exists, they can only address problems known by the user to exist.

Quantitative approaches on the other hand, are characterized by the use of independently objective measures for all risk metrics, including qualitative risk-metric descriptors such as "information asset", "threat", "vulnerability", and "safeguard/ controls" nomenclatures (Ozier 2003b:3).

According to Ozier (2003b:4) asset values are also expressed in monetary terms and threat frequency in annualised expressions that represent actual expected frequency (e.g., 1/10 for once in 10 years, or 50/1 for 50 times per year).

Although the opinion of the researcher is already been expressed in paragraph 4 under point 2.6, it still remains that quantitative approaches can lead to a reasonable result in prioritising and managing risk within a organization.

2.4.5 Example of how to develop a quantitative analysis model

Before a quantitative risk analysis model can be developed for security managers, it is essential to note that there are many types of models that are being used by analysts throughout the world. Some private companies and insurance companies make use of their own quantitative analysis models. Most of these models are solely based on the financial and engineering side. Some other models that exist, which are known to the researcher, is that of marketing, budgeting, transportation, facility and manufacturing models. In the security discipline, and mainly on quantifying physical risks according to different risk analysis concepts, no models exist which can be used as an instrument or tool for the security manager.

To prick the interest of the reader, the following discussion will be focussing on how to develop a quantitative analysis model.

It is important for the decision makers to involve a number of factors. For example, if one are considering looking at theft or fraud in a company, factors might include control measures, location and employees working in the company.

Before we consider an example, we must start by listing the factors and their relevant importance on a scale from 0 to 1.

A magazine distribution company has several branches spread all over the country.

The managing director aims to establish what the risk rating (high, medium or low) is regarding the different branches. The managing director has determined that the only three factors really important to him are control measures, location and employees. Furthermore the managing director decided that the location is the most important to him. He has given this a weight of 0.6. Employees are rated next with a weight of 0.3. Finally, the managing director has given control measures an importance weight of 0.1. As with any analysis of this kind, the importance weights for factors must sum to 1 (See Table 2.2).

Table 2.2: Factor weights

FACTOR	IMPORTANCE (WEIGHT)
Location	0.6
Employees	0.3
Control Measures	0.1

Source: Own compilation

Three branches were identified as an example and numbered branches 1 to 3. At this time the managing director feels comfortable with the factor weights.

Branch 1, location is given a weight of 0.7, employees an evaluation of 0.9 and control measures an evaluation of 0.6.

Branch 2 awarded a weight of 0.8 to location, 0.7 to employees and 0.8 to control.

Branch 3 awarded a weight of 0.9 to location, 0.6 to employees and 0.9 to control.

The results are shown in table 2.3

Table 2.3: Factor evaluations

FACTOR	BRANCH 1	BRANCH 2	BRANCH 3
Location	0.7	0.9	0.6
Employees	0.8	0.7	0.8
Control Measures	0.9	0.6	0.9

Source: Own compilation

Given this information, the managing director can determine a total weighted evaluation for each of the variables. Each branch is given a factor evaluation for the three factors, and then the factor weights are multiplied times the factor evaluation and summed to get a total weighted evaluation for each branch. As indicated in Table 2.4, branch 1 has received a total weighted evaluation of 0.75.

Table 2.4: Evaluation of branches

Branch Number	Factor name	Factor weight		Factor evaluation		Weighted evaluation
1	Location	0.6	x	0.7	=	0.42
	Employees	0.3	x	0.8	=	0.24
	Control Measures	0.1	x	0.9	=	0.09
	Total	**1**				**0.75**
2	Location	0.6	x	0.9	=	0.54
	Employees	0.3	x	0.7	=	0.21
	Control measures	0.1	x	0.6	=	0.06
	Total	**1**				**0.81**
3	Location	0.6	x	0.6	=	0.36
	Employees	0.3	x	0.8	=	0.24
	Control measures	0.1	x	0.9	=	0.09
	Total	**1**				**0.69**

Source: Own compilation

The same was done with Branch 2 who received a total weighted evaluation of 0.81. Regarding branch 3, the total weighted evaluation amounts to 0.69. The managing director must now take a decision on the highest total, which in effect means that the risk at branch 2 (0.81) is a high-risk area to operate in. This example of a very simple model can not only be used by managers, but also supervisors in the security industries to use as value-added services to their clients where services are rendered.

The problem with this type of model is that the probability and impact factors are not considered. It doesn't deal with the probabilities of future occurrences by analysing presently known probabilities.

Researcher undertakes in chapters 3 - 7 to develop and provide a quantitative analysis model by using risk analysis concepts, which can easily be used by security managers to identify and control risks within the organizational environment.

2.4.6 Advantages of quantitative modelling

There are a number of advantages of mathematical modelling such as the communication of problems and solutions to others. It can also save time and money in decision-making and problem solving. Researcher will briefly elaborate in this regard.

According to Render et al (2003:8-9) models can accurately present reality. Wayne and Albright (1997:4) agree but only if it is properly formulated. Models can help in the decision-making process. The decision maker can formulate problems such as risks facing his company.

Models can give insight and information especially when using the probability and impact in models. Models can also save time and money in decision-making and problem solving. According to Render et al (2003:9) it usually takes less time, effort and expense to analyze a model. To solve large or

complex problems in a timely fashion, it may be the only solution. A large company, for example, may literally experience high risks in the company, such as employee theft and fraud. To get the quickest and highest results in preventing such risks, a mathematical model may be the only option in determining the best solution that a company can achieve under these circumstances. Lastly, it can be said that the important advantage is to communicate problems and solutions to others. Render et al (2003:9) are of the opinion that a mathematical model can give direction to managers or executives in helping them make the final decision in solving problems.

2.5 EDUCATION OF THE SECURITY MANAGER IN QUANTITATIVE RISK ANALYSIS

The researcher established that no training in quantitative risk analysis exists for the private security manager, both internationally[15] and in South Africa.

According to Christman (2003b:4) training should be the key challenge. No longer can security companies hire someone and put them on assignment with only a new uniform and a pat on the back, especially when it's a managerial position. The belief of the public and organizational management is that giving private security personnel better training will make them not only a more effective crime fighting entity in future, but will enable them also to play a fundamental role in the total spectrum of risk management. To Spencer (1997:4) good training is essential, when you train people better, you also make an investment in them to get a higher return. The problem is that training costs money and companies and neighbourhoods that are hiring private security guards don't want to spend money (Spencer 1997:4).

The researcher is of the opinion that money be invested in training, especially in the training of private security managers, because a huge lack of training now exists, especially in the field of quantitative risk analysis. It serves no need for managers to be trained only in the general aspects of security but not being skilled in the total process of risk analysis and the normal security survey activities. Part of a security

manager's profile should contain the analysis of risk in order for them to assist their clients in the identifying of risk and the handling thereof. This can also be called a value-added service towards their clients.

In the researcher's own experience the modern private security manager should be able to demonstrate the following competencies:

- Knowledge of risk management functions;
- Conduct security risk analysis;
- Computer literacy;
- Knowledge of Occupational Health and Safety;
- Investigative skills;
- Language and communication proficiency;
- Designing and implementing awareness policies;
- Marketing;
- Knowledge of labour relations in security context;
- Design and implementation of contingency plans; and
- Apply business principles on the supervisory level of security practices.

It is becoming more and more apparent that security personnel and more specifically, security managers at all levels, need to have the necessary knowledge and skills to properly accomplish their main duty, namely the protection of personnel, property and assets.

The Private Security Industry Regulatory Act, Act 56 of 2001 is a legally established body regulating all private security companies in South Africa. It must be noted that from this legislation the Security Industry Regulatory Authority (SIRA) was born, which now controls and regulates the private security industry. Such companies therefore have to be registered with SIRA. Besides company registration, individual registration is also compulsory. An important prerequisite is the training of security officers. The general perception is that training, besides the actual security duty, is without a doubt the most extensive task in the security industry. Unsubstantiated

[15] *See schedules B and C*

information indicates that at any given time about 65% of all security personnel are either being trained or are involved in the planning and presentation thereof.
However, the facts obtained during researcher' interviews (See table 1.3), show that training in the security industry does not put enough emphasis on risk analysis in its curriculum, and it therefore impedes the objective of always ensuring the client of a high service standard. According to Eberlein and Karsten (1998:14) evaluation is a measurable standard, and can be viewed as feedback in order to implement the necessary changes. It is particularly vital for the security industry to follow the steps in the risk management process, namely risk identification, evaluation and management.

Valsamakis et al (2000:26) highlight that risk evaluation and analysis require specialist knowledge and techniques. The development of a risk analysis model therefore means that special skills and knowledge for general use in handling risks within an organizational context are required.

Risk analysis for the security industry in South Africa should therefore be one of the cornerstones on which successful training is built.

Hassenzahl (2002:12) states that a major problem is faced regarding the way analysis is used recently, keeping in mind how many well-developed methods and extensive quantitative and qualitative techniques exist. Unfortunately, much risk analysis seems to be handled quite badly due to a lack of knowledge and training in the field of risk analysis. According to Wold and Shriver (1997:9) security is an increasing concern and therefore it is of utmost importance that security managers be well educated in the aspects of risk analysis. Security managers should understand the following:

- How one can manipulate and critique a variety of risk analysis methods;
- How one can describe (quantitatively and qualitatively), manage and communicate uncertainty; and
- How others will interpret and use risk analysis processes and outputs.

Researcher agrees on what both authors are saying about education in this regard. Training in risk analysis should start at the security management level because they are the first line of defence in assisting their clients in the total spectrum of risk management. Risk analysis must therefore be the primary concern.

2.5.1 Involvement of security managers in quantitative risk analysis

Before a discussion on this topic can commence, it is necessary to give some statistics regarding registered security service providers in South Africa (See Table 2.5).

Table 2.5: Registered service providers per region

GAUTENG	1,674
MPUMALANGA	337
EASTERN CAPE	309
WESTERN CAPE	647
NORTHERN PROVINCE	253
FREE STATE	189
NORTHERN CAPE	57
KWAZULU NATAL	790

Source: Private Security Industry Regulatory Authority

According to SIRA, there are 210,924 registered and active security officers. Concerning inactive security officers the total amounts to 412,538. This brings the total active and inactive officers to 623,462. It is also established that there is no substantial evidence in proving how many private security managers are part of the total figure of 623,462, but unconfirmed information shows more or less a 12% of the total figure. It is therefore important that approximately 12% of security managers be familiar with all aspects concerning quantitative risk analysis and what it provides in the decision-making process.

According to Broder (2002:2) the one major resource required for risk analysis is trained manpower. During informal interviews with four of the twenty top ranking registered security providers in South Africa (see table 2.5), managers[16] indicated that no formal training exists in quantitative risk analysis.

During the researcher's informal interviews with some of the managers, he was especially shocked at the total absence of skills and knowledge regarding quantitative analysis. Some of the top management in these major security organizations is of the opinion that they are providers of a physical guard service, which do not, include any form of risk analysis training.

According to the security managers, this is more of a financial nature and security managers in general, are not financial professionals. Only a general security survey is carried out on demand and where necessary (See schedule D). If a need exists for a quantitative risk analysis, then they would rather call for outside advice. [17]

---

[16] *Informal interviews with some of the security managers indicated that they will provide information for this research project only on condition that their personal particulars are treated as confidential.*

[17] *Many companies call on outside consultants to perform studies, make evaluations, and offer recommendations for implementing or improving security programs. (Broder 2000:219).*

Even though security managers are not involved in the analysis process, they should be prepared to provide information assistance to those who might conduct it.

According to the interviewed managers, most of time they don't even know which risks or deviations to look for on their client's premises. One of the security managers, whose name is kept confidential for the purpose of this study, blames his top management for the lack of knowledge and training in the analysis field.

Information obtained during the interviews reveals that top management do not possesses the necessary skills to perform such an analysis and would therefore be putting their professional reputation on the line in ever admitting that they don't have the skills or knowledge in using a quantitative risk analysis model.

Taking the abovementioned discussion into consideration, the researcher is now more than ever convinced that security managers need intensive training on the whole subject of risk analysis.

According to the Private Security Industry Regulatory Authorities Training Division in South Africa, student security courses and/or modules for management (Grade A) don't contain any aspects on the total spectrum of risk analysis. In fact, no analysis courses from Grade A to Grade E are offered. The subjects for Grade A mainly focus on the following aspects:

- Basic principles of investigation;
- Action at the scene of an incident;
- Questioning of witnesses;
- Principles of giving evidence;
- Courts and court procedures;
- Human behaviour;
- Motivation and gaining co-operation;

- Report writing;
- Security registers;
- Interaction.

Enquiries at Technikon South Africa, also indicate that no subject on a physical quantitative risk analysis model for the private security exists. The division for security and safety management only focuses on the risk management discipline.

The success of any risk analysis undertaking should be strongly dependent on the role of top management in educating their managers. Taking this statement into consideration, the researcher strongly believes that he can contribute towards the development of an easy-to-use quantitative model in training the whole top management.

2.6 PROFESSIONALISM OF THE PRIVATE SECURITY MANAGER

As stated earlier, in this discussion, rendering a service in quantitative risks analysis for clients could not only add value to service but also sketch a portrait of professionalism.

According to Van Heerden (in Du Preez 1994:4), professionalism is inter alia, characterized by the following:

- Specialized knowledge and technical competency;
- Self discipline and self control;
- Commitment to an ideal of service;
- Peer group evaluation and peer group respect;
- Emotional neutrality (i.e. objectivity and stability);
- Clearly demarcated and permanent membership;
- General acceptance by the public that the occupation is in fact a profession.

Van Heerden (in Du Preez 1994:4) further contends that the security officer must satisfy some of the following requirements that are determinants of professionalism:

- Recognized professional status roles. Attaining a distinguished position which is recognized and respected by the community, employees and colleagues;
- Power. The ability/authority/competence to perform a professional task and to gain the desired result, regardless of the stumbling blocks;
- Skill. The capacity to perform difficult tasks;
- Responsibility. The responsibility for actions recognizes the accountability of the person concerned;
- Objectivity. A certain attitude projected by a member of profession who executes this task correctly, calmly, purposefully and in an unbiased way and does not allow external factors to influence own judgment;

Taking Van Heerden (in Du Preez's 1994:4) view about professionalism into consideration, it indicates that security managers should have a widespread of knowledge of security problems and how to handle them professionally. One way of doing this is that the security manager must be in a position to conduct a risk reduction analysis and to advise clients on various options to secure assets.

It is the researcher's view that the private security managers can contribute the same level of professionalism as their peers in various disciplines, such as human resource, legal, financial, and marketing managers.

2.7 LEGISLATIVE CONCERNS FOR PRIVATE SECURITY AND RISK ANALYSIS

Due to the booming of the private security industry in South Africa (researcher's own view) and the recognition by the state that it was performing duties, which was previously the responsibility of the state police a need arose to regulate the industry. In 1987, legislation in the form of the Security Officers Act (Act 92 of 1987) was passed by Parliament, which would regulate the private security industry in South Africa, which then allowed for the establishment of the Security Officers Board.

Thereafter in 1997 the legislation was amended and the Security Officers Amendment Act of 104 of 1997 was passed. The amendment provided for the establishment of an Interim Security Officers Board, which replaced the former SOB that was made up of people with vested interest in the industry.

The amendment of the 1987 Act (Act 92 of 1987) and the appointment of an interim SOB has to be seen against the background of problems experienced by the old SOB. The industry was plagued by infighting and allegations of nepotism and corruption.

The Security Officers Amendment Act of 104 of 1997, stipulated the appointment of an interim SOB and tasked the Minister for Safety and Security with drafting legislation within a period of eighteen months for the purpose of evaluating current regulation of the industry, and suggesting a new regulatory framework, where appropriate. Further more, the interim board is mandated to conduct an internal review of the regulatory affairs of the board such as, inter-alia, administration and staffing, and submit recommendations to the Minister of Safety and Security for his consideration. Some of the main functions of the board are:

- Registration and maintenance of a computerized data base consisting of all registered security officers and security businesses;
- Fingerprint classification;
- Setting training standards;
- Inspection and prosecution of security businesses breaking the law;
- Drafting of legislation and amendments of the Security Officers Act.

Without proper regulation there will be chaos in the security industry, which could interfere and/or damage the rights and interests of the public, employee security officers and law-abiding security businesses will not be sufficient protected.

Further tightened regulatory measures were implemented with the commencing of the new, so-called “PSIRA” Act, that was passed on 14 February 2001. This is called the Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001).

This Act now places the emphasis on the following aspects:

- The scope of regulation (who and what will be regulated);
- The nature and scope of the body that will direct regulation (who will regulate);
- The exact principles and methods to be used in regulating the industry in future (how regulation will work in practice).

Besides the abovementioned legal concerns for the private security industry, one of the most commonly asked questions regarding the analysis process within companies surrounds its legal enforceability. Although the King II guidelines on corporate governance focuses mainly on operational risks, it is researcher's view that physical risks also requires a system that is embedded in the operations of the organization and is capable of the kind of response that provides accurate root cause risk analysis. The King II report is not legislation and as such does not have the binding effect of legislation. The report is in essence a code, designed to give guidelines for good corporate governance (King 1994:1).

The Company Act, Act 61 of 1973 governs all companies. The Act contains various sections that fall within those requirements contained in the report. One section is the management function, which automatically includes risk management[18]. The analysis process forms part of any management function and is therefore necessary in developing a successful growing business. The emphasis is placed on "any management" which includes security management.

Contractors Regulations as per Government Notice 25207 of 2003 now also place the emphasis on risk analysis[19]. Regulation 7 (1) state clearly that every contractor performing construction work shall, before commencement of any construction work and during construction work, cause a risk assessment to be performed by a

---

[18] *Risk Management process entails the planning, arranging and controlling of activities and resources to minimize the impacts of all risks. (King 1994:97). This means that risk analysis should form part of the overall planning process within companies.*

[19] *According to Government Notice 25207 of 18th July 2003, risk analysis is defined as a program which determine any risk associated with any hazard at a construction site, in order to identify the steps needed to be taken to remove, reduce or control such hazard.*

competent person appointed in writing and the risk analysis shall form part of the health and safety plan to be applied on the site and shall include at least:

- The identification of the risk and hazards to which persons may be exposed to;
- The analysis and evaluation of risks and hazards identified;
- A documented plan of safe work procedures to mitigate, reduce or control the risks and hazards that have been identified;
- A monitoring plan; and
- A review plan.

Regarding the above discussion it is clear that the private security manager has a fundamental role to fulfil in the total spectrum of security, risk management and risk analysis, which is legally driven.

2.8 THE FUTURE OF THE PRIVATE SECURITY AND QUANTITATIVE RISK ANALYSIS

Private security has come a long way. Developments in governmental regulations have resulted in restructuring of the Industry and standards to create improvements in the quality of personnel, education and training needed to promote a positive view of the private security industry.

The researcher estimates that the average annual rate of growth of the private security industry's personnel to the year 2010 will be approximately 7% per year. The reason for this viewpoint is that (i) companies focussing on the outsourcing of departments that is not the core business of a their companies, such as in house security (ii) concern that businesses may be vulnerable to crime (iii) a need to comply with new mandates from insurance companies and (iv) a desire to have the kind of 24 hour presence that police officers don't have time to devote to one particular business or neighbourhood. One can quickly realize the potential available for an individual thinking of a career in the private security industry (Hall 2003:5).

For the management of the private security industry, it is essential that managers not only be educated in the general aspects of security, but also in the risk analysis process, as this forms part of any management function (see point 2.12). Tools, such as, the "TIQCAM" model (see point 7.1 and footnote 18) can be used with great success to expose physical vulnerabilities. We have to remember that we cannot be lax in security by just patching what we think is wrong. A tool such as the "TIQCAM" model reminds us that we sometimes need to view things from another angle, such as, the quantifying of risk, in order to present the full picture to our clients.

Although quantitative risk analysis for the private security industry is not a primary issue, it will not only expand in the near future and encourage the private security manager to be better educated in risk analysis, but will also boost the professional image of the whole private security industry.

It is also the researcher's view that the in-house security managers will also benefit from the use of a quantitative risk analysis model in the future.

2.9 CONCLUSION

The private security industry continues to grow with the demand for more guards, which also means the possible promotion of some of these guards to positions such as managers. This is where private security providers need to dedicate themselves and their managers to education regarding quantitative risk analysis, by using a suitable model. This will not only label them as professional private security providers but will also lead to the decreasing of risks.

From the aforementioned discussion, the following chapter will focus solely on the steps in developing a quantitative risk analysis model for the private security manager.

CHAPTER 3

THE PROBABILITY CONCEPT WITHIN THE RISK ANALYSIS APPROACH

3.1 INTRODUCTION

Private security managers are involved in the day-to-day security risk quantification and therefore will not be fully acquainted in dealing with the different concepts in risk analysis. Their roles are primarily based on the identification of risk and the implementation of suitable control measures.

The purpose of this chapter is to expose the private security manager to the first concept, “probability”. Understanding this concept will not only help the security manager, but also decision makers in choosing wisely under conditions of uncertainty. Probability is the language of uncertainty (Schuyler 2001:141).

According to Render et al (2003:78) the successes or failures that persons experience in life depend on the decisions that they make. Risk communication[20] characterizes and presents information about security risks and uncertainties to decision-makers.

The quantification of any risk is mainly based on three types of concepts (probability, impact and cost of risk) used in determining the outcome or seriousness of that risk. For this discussion, the focus will be on the probability concept.

3.2 PROBABILITY CONCEPT AND APPLICATION

A brief discussion on the probability concept clarification was presented under point 1.6.6 with the aim of attracting the interest of the reader. Although much could be written and said about this concept, this discussion will be of a more focussed nature regarding the application in quantifying risk. For the purpose of introducing "probability", the researcher is of the opinion that only the following aspects are important and applicable to this study.

3.2.1 A short history of probability

Apostol (1969:1) drew the attention to gambler's dispute in 1654 that led to the creation of a mathematical theory of probability by two famous French mathematicians, Blaise Pascal and Pierre de Fermat.

Chevelier de Méré, a French nobleman with an interest in gaming and gambling questions, called Pascal's attention to an apparent contradiction concerning a popular dice game. The game consisted of throwing a pair of dice 24 times; the problem was to decide whether or not to bet even money on the occurrence of at least one "double six" during the 24 throws. A seemingly well-established gambling rule led De Méré to believe that betting on a double

[20] *The word communication is derived from Latin "communicare", meaning common, to share, indicating a process having joint action as its purpose. To communicate with somebody is a complex process where many factors influence the outcome (Reksness 2003:1).*

six in 24 throws would be profitable, but his own calculations indicated just the opposite.

This problem and others posed by De Méré led to an exchange of letters between Pascal and Fermat in which fundamental principles of probability theory were formulated for the first time. Although some Italian mathematician had solved a few special problems on games of chance in the 15^{th} and 16^{th} centuries, no general theory was developed before this famous correspondence.

Since then the ideas have been refined somewhat and probability theory is now part of a more general discipline known as the measure theory.

3.2.2 Types of probabilities

Where do probabilities come from? According to Render et al (2003:36) sometimes they are subjective and based on personal experiences. Other times they are objectively based on logical observations such as the roll of a dice. Often, probabilities are also derived from historical data.

- Objective approach

  The following objective approach by Glosser (1999:1) is based on the fact that the study of probability helps us figure out the likelihood of something happening. For instance, a spinner has 4 sectors coloured yellow, blue, green and red. What are the chances of landing on blue after spinning the spinner?

  The chances of landing on blue are 1 in 4, or one fourth. The problem in Glosser's (1999:1) theory was to find the probability that the spinner will

land on blue. Table 3.1 highlights the definitions and examples from the problem.

Table 3.1: Definitions and examples

Definition	Example
An **experiment** is a situation involving chance or probability that leads to results called outcomes	The **experiment** is spinning the wheel
An **outcome** is the result of a single trial of an experiment	The possible **outcomes** are landing on yellow, blue, green occurred
An **event** is one or more outcomes of an experiment	The **event** being measured is landing on blue
Probability is the measure of how likely an event is	The **probability** of landing on blue is one fourth

Source: Glosser (1999:1)

In order to measure probabilities, mathematicians have devised the following formula for finding the probability of an event (see table 3.2).

Table 3.2: Formula for finding probability of event

Probability of an event
$P(A) = \frac{\text{The number of ways event can occur}}{\text{The total number of possible outcomes}}$

Source: Glosser (1999:1)

The probability of event A is the number of ways event A can occur divided by the total number of possible outcomes. According to Glosser (1999:2) a slight modification of the problem is as follows:

Experiment:

A spinner has 4 equal sectors coloured yellow, blue, green and red. After spinning the spinner, what is the probability of landing on each colour?

Outcomes:

The possible outcomes of this experiment are yellow, blue, green and red.

Probabilities:

$$P(\text{Yellow}) = \frac{\text{number of ways to land on yellow}}{\text{total number of colours}} = \frac{1}{4}$$

$$(\text{Blue}) = \frac{\text{number of ways to land on blue}}{\text{total number of colours}} = \frac{1}{4}$$

$$(\text{Green}) = \frac{\text{number of ways to land on green}}{\text{total number of colours}} = \frac{1}{4}$$

$$(\text{Red}) = \frac{\text{number of ways to land on red}}{\text{total number of colours}} = \frac{1}{4}$$

Taking the above simple example into consideration, the probability of occurrences can be expressed as a fraction or a decimal from 0-1.[21]

Therefore a basic understanding of probability makes it possible to understand everything from the weather report averages to your chances of being struck by lighting, or in the contemporary situation in South Africa, being a victim of hi-jacking. Probability is an important topic for mathematics because the probability of certain events happening or not happening can be as important to them as in the real business world.

- Subjective approach

[21] *See chapter 1 (point 1.6.6)*

When logic and history are not appropriate, probability values can be assessed subjectively. According to Render et al (2003:36), the accuracy of subjective probabilities depends on the experience and judgment of the person making the estimates. A number of probability values cannot be determined unless the subjective approach is used. What is the probability that crime will be severe in 2010? What is the probability that you will be president of a major corporation in five years? (Mun 2002:2).

There are several methods for making subjective probability analysis according to Render et al (2003:36). Opinion poles can be used to help in determining subjective probabilities for possible election returns and potential political candidates. In some cases, experience and judgment must be used in making subjective analysis of probability values (Render et al 2003:36).

3.2.3 Risk Matrix

Martin and Tate's (2002:6) perception of risk matrix is a table used to assign a "score" to the identified risk, to assist with the risk management process. In fact, it is the core of the risk management documentation. For each risk identified, a score is assigned for the probability and impact[22] aspects.

Often a range of 1-5 is used for each aspect. Different organizations use different ratings. To Render et al (2003:34) the rules regarding the probability rating is 0-1 (see point 1.6.6).

Concerning the ratings of probability, some authors, Render et al (2003:34), Wayne and Albright (1997:499) and Martin and Tate (2002:2) share the same view but with a slight difference in expressions. For the purpose of this

[22] *See discussion of impact risk ratings in Chapter 4.*

discussion, the researcher will abide by the latter view which are given below in table 3.3:

Table 3.3: Probability risk rating

Probability rating	**Level of probability**	**Definition**
Zero	Zero	No chance that the risk will occur
.1	Very low	Probability that this event will occur is between 1-20%
.3	Low	Probability that this event will occur is between 21-40%
.5	Medium	Probability that this event will occur is between 41-60%
.7	High	Probability that this event will occur is between 61-80%
.9	Very high	Probability that this event will occur is between 81-99%
1.0	Certainty	If the probability of occurrence is 100% then that means it is not a risk but an assumption

Source: Martin and Tate (2002:2)

Mun (2000:3) states that a risk management integrated team typically completes a risk matrix. The approach for such a team before commencing in rating the probability of any event is as follows:

- List every risk identified;
- For each risk, estimate probability and impact;
- Calculate overall rating (probability and impact);
- Identify detailed risk mitigation (reduction) strategies;
- Optionally, estimate "net" risk rating (after allowing for effect of mitigation strategy.

A risk management integrated team should include risk management specialists such as a risk manager (in some instances also known as the security manager) or a risk analyst consultant. Businesses normally direct the risk issues to their risk management and or risk control department. This is where the security manager and or risk manager must know the full spectrum of the risk analysis approach (see figure 1.1.). A discussion on the risk analysis approach is vital in understanding that quantitative approach consist of concepts which must be taken into consideration such as the probability concept.

3.3 DEVELOPMENT OF THE "TIQCAM" MODEL

The "TIQCAM" model (researcher's own design) starts of with a risk problem, which will lead to the commencement of a quantitative risk analysis. In doing a risk analysis the analyst should take all the different concepts into consideration. These concepts have their own criteria, which are important in the analysing process to come to a positive result regarding the risk problem.

These concepts are illustrated in figure 1.1 which follows the following steps:

- Step 1: Probability
- Step 2: Impact
- Step 3: Cost factor

- Step 4: Degree of correction
- Step 5: Human factor

After all the steps are taken into consideration, it will then reflect the risk subtotal and the risk total where after a risk classification will be established. This classification plays a fundamental role in the whole analysing process because it will then determine if future action is needed. This also means that the future action must then be taken into consideration for decision-making purposes in solving the risk problem. The future action is thus illustrated in figure 1.1 with a red connection line to place the emphasis on the importance in solving the risk problem.

For example, the following discussion regarding the different steps in the approach to developing of the foresaid model, researcher will stick to the use of a magazine distribution company as used under point 2.3.5. Furthermore, the researcher will only use two physical risk problems, namely robbery and fraud –which is a sensible approach because they (the risks) probably represent the gambit of speculative risks to any enterprise : violence and stealth, as an example to establish the end result of that risk problem, bearing in mind that in developing this model, the researcher is going to use hypothetical ratings which will be assigned to the two foresaid risk problems in order to come to the risk classification. This will give the reader a better insight in how to use the model in a practical way.

3.3.1 Integrating the probability concept as step one (1) in the development process

With reference to point 1.6.6, the researcher is of the opinion that the probability concept plays an important role in the starting point of this model development. It must also be clearly understood that although there can be written and debated widely concerning this concept, this model development is an “easy-to-use” model for private security industry and might easily be used by some other disciplines in the business world.

With reference to the concept “probability”, three aspects are taken into consideration, namely the criteria aspects, risk indicator and the risk rating.

3.3.1.1 Criteria

Although analysts use different criteria, the following is applicable for the purpose of this study.

- Event will occur is between 81% and 100%
- Event will occur is between 61% and 80%
- Event will occur is between 41% and 60%
- Event will occur is between 21% and 40%
- Event will occur is between 1% and 20%

3.3.1.2 Risk indicator

To establish what the risk indicators are in relation to the different foresaid criteria; it is necessary to reflect it towards these different criteria.

Criteria	Risk indicator
• Event will occur between 81% and 100%	Certainty
• Event will occur between 61% and 80%	High
• Event will occur between 41% and 60%	Medium
• Event will occur between 21% and 40%	Low
• Event will occur between 1% and 20%	Very low

3.3.1.3 Risk rating

It is important that every risk indicator must have a risk rating in order to come to a positive rating of the risk problem.

Risk indicator	Risk rating
• Certainty	1.0
• High	.7
• Medium	.5
• Low	.3
• Very low	.1

It is now necessary to combine the probability concept aspects in table form as illustrated in table 3.4. As mentioned earlier on, hypothetical ratings are being used.

Table 3.4: Combined illustration of probability aspects

Risk problem	Criteria	Risk indicator	Risk rating
Robbery	Event will occur between 41% and 60%	Medium	.5
Fraud	Event will occur between 81% and 100%	Certainty	1.0

Source: Own compilation

3.4 CONCLUSION

This chapter outlined the importance of the probability concept as the first step in the developing of a quantitative analysis model. Security managers must always bear in mind that they can do a lot with probabilities. It also gives a solid foundation on which the manager may base his recommendations for corrective actions. Probability is thus the language of uncertainty and is very important in the decision making process (Schuyler 2001:141).

From the abovementioned discussion, the following chapter will not only address the second step in the “TIQCAM” model approach, namely the impact concept, but will also involve a joined Excel formulation with the probability concept. The same strategy will be applied to all the concept chapters that will follow. The idea is to ease the discussion to the end (Chapters 3 to 7) to totally complete the development of the “TIQCAM” model in chapter 7, by reaching an exact risk classification regarding the risk problem as indicated in table 3.4.

CHAPTER 4

INTEGRATIVE APPROACH OF THE IMPACT CONCEPT IN BUSINESS IMPACT ANALYSIS

4.1 INTRODUCTION

In this discussion the impact concept forms part of step two (2) as illustrated in figure 1.1. This concept plays a vital role in the risk analysis process and, according to the researcher, is built on two main pillars, namely: sensitivity[23] and severity[24]. These two elements will each have their own criteria, risk indicators and values when discussing it as part of the development of the model under point 4.4.

The major risk in South Africa is crime, which has a tremendous impact on the whole of South Africa's citizenry. Businesses are also touched by the high rate of crime and therefore must lower the risk by impact analysis.

This chapter aims to elaborate more on the impact concept clarification as mentioned in chapter one (point 1.6.9) to enable the security manager to understand the bigger picture. It will also address the fact that the impact concept can not function in isolation. The other concepts, such as probability, will also play a vital role in the outcome of the end result in developing the "TIQCAM" model.

4.2 CLARIFICATION OF THE CONCEPT IMPACT

In Chapter one under point 1.6.9, the impact concept was briefly discussed with the aim to lay the foundation or basis for deeper analysis. Bearing in mind the different

---

[23] *According to the Pharos Dictionary, sensitivity can be defined as the quality or state of being sensitive. It can also be the ability to respond to physical stimuli or to register small physical amounts. Also a state which can course embarrassment*

[24] *Situation of seriousness according to the Pharos Dictionary.*

views of authors concerning the business impact analysis (BIA), it will then be safe to define impact of disruption over time and assist in the understanding of the amount of risk to assume, transfer or mitigate. A common question normally asked by security managers and business continuity planners are: How much reduction in premium can we expect from our insurance company if risk control programs are in place? The answer is usually not much, especially when compared to the probable maximum loss, which can be avoided if the appropriate programs and resulting mitigations are in place (Kruger 2003:3).

According to Broder (2000:108) a risk analysis and a business impact analysis can greatly reduce the cost of insurance by identifying and quantifying a potential loss, thereby allowing the security manager to avoid over or underinsuring the risk.

Broder (2000:108) is further of the opinion that BIA will allow management to make timely decisions about future business issues, and it will help the organization avoid a less than speedy recovery.

Broder (2000:108) strongly places the emphasis on the BIA, which will help to:

- Identify which processes and computer applications are critical to the survival of the organization;
- Establish the value of each business unit as it relates to the whole, not to itself;
- Identify critical resources of the organization;
- Gain support for the recovery process from senior management;
- Increase management's awareness of the issues and resources required for a workable program, as well as introduce a basic planning structure to the management group;
- Potentially reveal inefficiencies in normal operations;
- Help to justify or allocate better recovery planning budgets (cost/benefit).

4.3 INTERACTION BETWEEN THE IMPACT AND PROBABILITY CONCEPTS

The researcher is of the opinion that to achieve the most accurate risk-rating outcome, the impact concept in any risk analysis cannot be seen in isolation. The probability rating also plays a vital role in establishing the correct measurement in the analysis process. You should then consider the risk rating as being:

The impact x the probability

The researcher's perception is also that there is no standard way of measuring the impact or probability of a risk. It is up to the risk and/or security practitioner to consider and prioritise this risk in his own manner.

Martin and Tate (2002:3) use a risk analysis matrix (see table 4.1) to enter the rating for the probability (P) of the risk occurring in the "P" column. Consider how likely it is that this risk will happen in terms of the specific nature and context of the project.

Table 4.1: Risk Analysis Matrix

Potential risks	**Probability / Impact ratio**	**Controls / Risk mitigation**
	P **I** **P x I**	

Source: Martin and Tate (2002: 5)

Record the rating of the impact (I) of the risk should it occur in column "I" on the matrix. This enables analysis of the effect this risk will have if it occurs on the achievement of the aims and objectives of the project according to Martin and Tate (2002:3).

To calculate the impact/probability ratio (PI), multiply the scores in each column (P x I) to combine the likelihood of the risk occurring with the consequence. The score is rated on a scale of 0-10 with 0 being the lowest probability/impact (PI) ratio. Therefore the highest PI ratio score possible is 1 (Martin & Tate 2002:3).

Identified potential risks should be analysed, with a tentative indication of the significance of each risk (clearly significant; PI score above 7.5, possible significant; PI score above 5.5, and probably insignificant; PI score under 3.5) and inter-relationships between risks. A sample of an impact risk-rating is shown in table 4.2 below.

Martin and Tate (2002; 3) state further that if a risk is related to one or more other risks, in the sense that they share common causes or for other reasons, the occurrence of one affects the likelihood of another, the related risks should be evaluated together. The resulting analysis of each risk or group of related risks should be entered in the risk matrix.

The significance of risks should be reviewed and then they should be reclassified into the categories of significance. For risks, which are probably insignificant (i.e. low score on PI ratio), the decision must be made as to whether they can be ignored or not according to Martin and Tate (2002:3).

Table 4.2 Impact risk rating

Impact rating	Level of impact	Meaning
0 (Zero)	0 (Zero)	There is no impact if the risk should occur. Therefore, it's not truly a risk
1.5	Very low	The impact is minor
3.5	Low	The impact is minor but would be noticed by the customer, and would create minor customer dissatisfaction
5.5	Medium	The impact on the company or project is not insignificant and would create dissatisfaction.
7.5	High	The impact is significant and would create major dissatisfaction. It could jeopardize the company or the project.

9.5	Very High	The impact is catastrophic and would kill the project.

Source: Martin and Tate (2002:2)

Particular attention and care must be taken in identifying and classifying risks that could have either:

- Serious or catastrophic consequences or high expected values; or
- Exceptionally favourable consequences.

All the risks in both of these categories are likely to need particular, individual attention when analysing the overall "riskiness". A decision must be made about which risks are amenable to more detailed evaluation and quantification (Martin & Tate 2002:4).

4.4 INTEGRATING THE IMPACT CONCEPT AS PART OF THE DEVELOPMENT OF THE "TIQCAM" MODEL

Risk impact, as the second step (see figure 1.1) in the developing of the "TIQCAM " model, plays a vital role in the quantitative risk analysis process and, according to the researcher, is built on two main pillars, namely: sensitivity and severity. These two elements will each have their own criteria, risk indicators and values.

4.4.1 Sensitivity

The focus here is on outside factors such as the media, public and local concern as described in the criteria below. Media propaganda can have a great and sometimes negative impact on the business environment when accidents occur.

Criteria

- Media event, immediate broad concern
- Media event
- Local concern

- Public concern
- No public concern

Risk indicator

To establish what the risk indicators are regarding the different aforementioned criteria, it is necessary to reflect it towards the different criteria as stipulated below.

Criteria	Risk indicator
Media event, immediate broad concern	Catastrophic
Media event	Major
Local concern	Moderate
Public concern	Minor
No public concern	Insignificant

Risk rating

It is important that every risk indicator must have a risk rating in order to come to a positive rating of the risk problem.

Risk indicator	Risk rating
Catastrophic	5
Major	4
Moderate	3
Minor	2
Insignificant	1

4.4.2 Severity

The following criteria are applicable to the term severity.

Criteria

- Multiple deaths, or damages over R6 000 000
- Single death or multiple injuries or damages between R4 000 000 and R5 000 000
- Individual injuries, loss or damages R3 000 000
- First aid, loss or damages R2 000 000
- No injuries and/or minor loss and damages

Risk indicator

To establish what the risk indicators are regarding the different foresaid criteria, it is necessary to reflect it towards the different criteria as stipulated below.

Criteria	Risk indicator
Multiple deaths, or damages over R6 000 000	Catastrophic
Single death or multiple injuries or damages between R4 000 000 and R5 000 000	Major
Individual injuries loss or damages R3 000 000	Moderate
First aid, loss or damages R2 000 000	Minor
No injuries and or minor loss and damages	Insignificant

Risk rating

It is important that every risk indicator must have a risk rating in order to come to a positive rating of the risk problem.

Risk indicator	Risk rating
Catastrophic	5
Major	4
Moderate	3
Minor	2
Insignificant	1

Putting the abovementioned discussion in perspective, the sensitivity and severity aspects of the impact concept forms part of a combination illustration as per table 4.3.

Table 4.3: Combined illustration of risk impact aspects

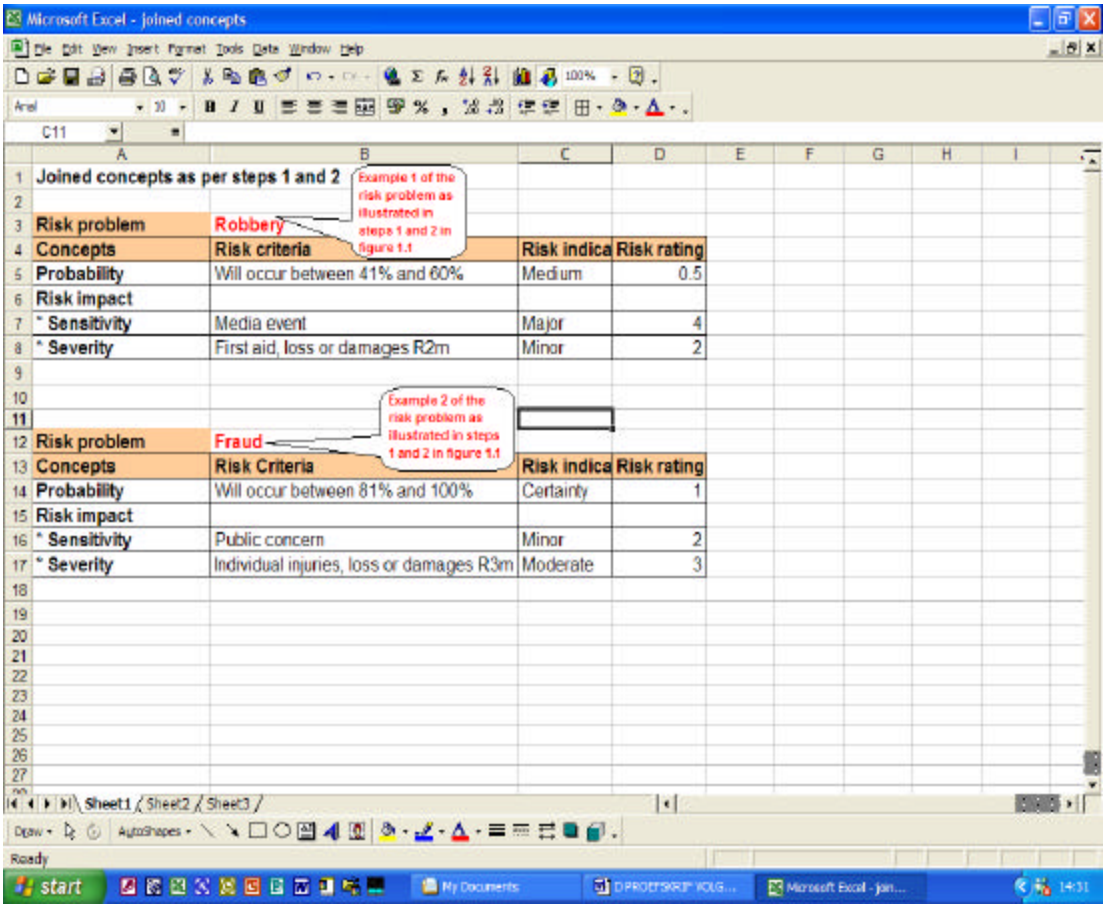
SENSITIVITY				SEVERITY		
Risk problem	**Criteria**	**Risk indicator**	**Risk rating**	**Criteria**	**Risk indicator**	**Risk rating**
Robbery	Media event	Major	4	First aid, loss or damages R2 000 000	Minor	2
Fraud	Public concern	Minor	2	Individual injuries, loss or damages R3 000 000	Moderate	3

Source: Own compilation

4.5 JOINED PROBABILITY AND IMPACT CONCEPTS IN EXCEL FORMAT

It is important that the concepts as per tables 3.4 and 4.3 now be illustrated in Excel spreadsheet format as suggested in chapter 1 under point 1.6.3. The foresaid concepts in tables 3.4 and 4.3 are joined together in order to give the reader a better picture of the model appearance so far (see figure 4.1).

Figure 4.1: Probability and impact concepts joined in Excel format



Source: Own compilation

4.6 CONCLUSION

Taking the abovementioned discussion into consideration, it is clear that the impact and the probability concepts are not enough to really participate in the exact quantitative outcome of a risk problem. To achieve a high level of reliability and also to strengthen the development of the "TIQCAM" model, it is necessary to integrate the cost factor concept in this process. The latter concept can support a solid basis upon which decisions can be based.

The following chapter will address the cost factor concept as step three in the "TIQCAM" model as illustrated in figure 1.1.

CHAPTER 5

ESSENTIALITY OF THE COST FACTOR IN RISK MEASURING

5.1 INTRODUCTION

The cost factor can be considered as the essential and dynamic part of the risk analysis process. Costs of high risk can have a definite impact on an organisation's growth and development. The cost factor must therefore also integrate the degree of correction concept (see chapter 6) in lowering the costs of risk by means of implementing some protection measures.

Attention will be given in this chapter to the cost factor and its application. Thereafter the development of the "TIQCAM" model comes under the loop with the cost factor integrated with the concepts, probability and impact. Lastly, joined concept illustration in Excel format involving the cost factor concept will be presented.

5.2 COST FACTOR CONCEPT AND APPLICATION

In the introduction to this chapter it was said that it is essential for the private security manager to bear in mind that cost of threats can in some instances be more expensive than the value of an asset. It is therefore of utmost importance to quantify the threats and/or risks in an attempt to find the most cost effective measures of protecting the company's assets.

To do this, it is important to identify which threats will be dealt with and how. According to Shimonski (2002:3) decisions will need to be made by management as to how to proceed, based on the data that is collected regarding the risks. In most cases, this will involve devising methods of protecting the asset from threats. This may involve installing security software, implementing policies and procedures, or adding additional security measures to protect the asset.

Shimonski (2002:3) is further of the opinion that one may decide that the risks involved in an asset are too high, and the cost to protect it are too high as well. In such cases, the asset should be moved to another location, or eliminated completely. For example, if there is a concern about a Web server affected by vibrations from earthquakes in California, then moving the Web server to the branch office in New York nullifies the threat. By removing the asset, you subsequently eliminate the threat of it being damaged or destroyed (Shimonski 2002:3).

The researcher agrees with Shimonski (2002:3), but is of the opinion that transferring the loss to another party, such as the insurance companies, the company can also benefit in a way by not being solely responsible for an asset loss. When a loss occurs, the company can be reimbursed. Leasing equipment can also be an additional option in that the responsibility of cost is transferred to the leasing company to replace or fixing assets involved.

As in the case of the risk ratings for the probability and impact concepts, it is also necessary to indicate the score of "cost of risk" by means of a cost of risk rating. Fine (1991:80) indicates that the only way to determine whether proposed corrective action to alleviate a risk situation is justified, the estimated cost of the corrective measures is balanced or weighed against the degree of risk. Integrating two additional factors into the risk score formula as follows does this:

Justification = Cost Factor x Degree of Correction

The cost factor according to Fine (1991:80) is a measure of the estimated dollar cost of the proposed corrective action (see table 5.1).

Although the researcher agrees with Fine (1991:80) on his two additional concepts, it appears that he only multiplied the cost of risk and degree of correction and then came to a probable score which then indicates that a risk is high, medium or low.

Table 5.1: Cost of risk rating in Dollars

Cost	Rating
Over 50 000 dollar	10
25 000 to 50 000 dollars	6
10 000 to 25 000 dollars	4
1 000 to 10 000 dollars	3
100 to 1 000 dollars	2
25 to 100 dollars	1
Under 25 dollars	0.5

Source: Fine (1991:80)

If one looks at Fine's (1991:80) justification formula which divides the Impact x Probability by the Cost of Risk x Degree of Correction, it should also make provision to subtract the Degree of Correction from the Cost of Risk, in setting a more reliable risk score for decision making purposes, which is not the case in Fine's (1991:80) description of his model.

In the researcher's development of a quantitative risk analysis model (see chapter 7) he also based his formula on Fine's principle (1991:80) but with a difference in the risk rating. Fine (1991:80) rated his highest score on 10 with the lowest score as 0.5, whilst the researcher's scores are rated on a scale between 1-5 (See table 5.2).

Table 5.2: Cost of risk rating in Rand

Cost	Value
Loss more than R 8 000 000	5
Loss between R 6 000 000 to R 8 000 000	4
Loss between R 4 000 000 to R 6 000 000	3
Loss between R 1 000 000 to R 3 000 000	2
Loss under R1 000 000	1

Source: Own compilation

The reason for the difference in risk ratings as per tables 5.1 and 5.2 is that authors, such as Martin and Tate, Render et al, and Wayne and Albright also differ when it comes to the calculation of risks. In the researcher's view, risk ratings are not always

exact, but at least gives a clear indication to the companies' executives of how serious their risks must be before giving their full attention to mitigating them.

5.3 INTEGRATING THE COST FACTOR CONCEPT AS PART OF THE DEVELOPMENT OF THE "TIQCAM" MODEL

The approach regarding the cost factor as step 3 in the development process, is to determine the financial loss a company could experience due to its risk situation. This is accomplished by looking at the criteria, risk indicator and the risk rating.

5.3.1 Cost Criteria

The following criteria are applicable as follows:

- Loss more than R8 000 000
- Loss between R6 000 000 and R8 000 000
- Loss between R4 000 000 and R6 000 000
- Loss between R 1 000 000 and R3 000 000
- Loss under R1 000 000

5.3.2 Cost Risk Indicator

The cost risk indicator will be reflected according to the cost criteria.

Cost Criteria	Cost Risk Indicator
• Loss more than R8 000 000	Certainty
• Loss between R6 000 000 and R8 000 000	High
• Loss between R4 000 000 and R6 000 000	Medium
• Loss between R 1 000 000 and R3 000 000	Low
• Loss under R1 000 000	Very low

Cost Risk Rating

It is important that every risk indicator must have a risk rating in order to come to positive rating of the risk problem.

Cost Risk Indicator	Cost Risk Rating
Certainty	5
High	4
Medium	3
Low	2
Very low	1

It is necessary to combine the cost factor concept aspects in table form as illustrated in table 5.3.

Table 5.3: Combined illustration of the cost factor aspects

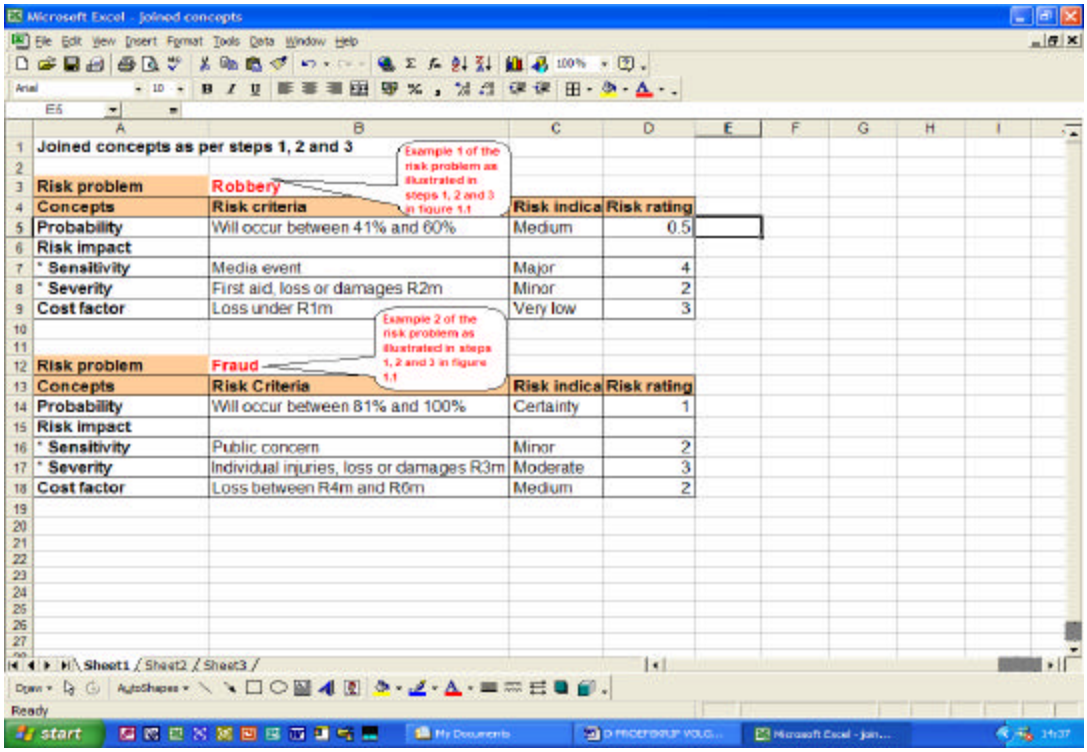
Risk problem	Cost criteria	Cost risk indicator	Cost risk rating
Robbery	Loss under R1 00 000	Very low	1
Fraud	Loss between R4 000 000 and R6 000 000	Medium	3

Source: Own compilation

5.4 JOINED COST FACTOR, IMPACT AND PROBABILITY CONCEPTS IN EXCEL FORMAT

The cost factor concept as indicated in table 5.3 is joined with the impact and probability concepts as reflected in figure 5.1 below.

Figure 5.1 : Cost factor concept joined in Excel format



Source: Own compilation

5.5 CONCLUSION

For any company executive, the financial implications regarding any risk situation are of utmost importance. Quantitative risk analysis can be a helpful tool in accurately establishing the cost of risk, taking the degree of correction (physical protection measures) into consideration.

In researcher’s earlier discussion (point 5.2) it seems that, as in the case of the probability and impact concepts that the cost factor can also not function in isolation. The cost of any risk should be weighed against the degree of correctional steps that might already be implemented in a company.

CHAPTER 6

DEGREE OF CORRECTION AS A MITIGATIONAL CONCEPT IN THE ANALYSIS PROCESS

6.1 INTRODUCTION

As step four in the analysis, the degree of correction plays a fundamental role in achieving the most accurate risk rating outcome in developing the "TIQCAM" model

This concept mainly focuses on the mitigation aspect in the risk analysis process by taking all the necessary physical protection measure into consideration (e.g. guards, camera's, fences, etc.). This can have a definite influence on the cost factor and the final risk classification.

As with the interaction between the probability and impact concepts (See point 4.3), the degree of correction can also not function in isolation and must therefore be integrated with the cost factor. The reason for this is that the degree of correction has a definite influence on the cost of an organisation.

This chapter aims to elaborate more on the degree of correction's role in the risk analysis process and its combination with the cost of risk factor.

6.2 DEGREE OF CORRECTION CONCEPT IN THE DEVELOPMENT OF THE "TIQCAM" MODEL

Before one can establish the real cost of a risk, it is necessary to look at the degree of correction, which means that safeguarding and/or control measures must first be taken into consideration. Once this is done, the percentage of existing correction (see table 6.1) must then be subtracted before the degree of correction can be multiplied by the cost of risk.

Table 6.1: Degree to which control measures are in place

Classification	Rating
100% control measures in place	1
At least 75% control measures in place	2
Control measures between 50-75% in place	3
Control measures between 25 to 50% in place	4
Less than 25% control measures in place	5

Source: Own compilation

The estimated cost of a risk must be balanced against the degree of correction by means of determining the physical control measures implemented. This is also accomplished by looking at the criteria, risk indicator and the risk rating.

6.2.1 Degree of Correction criteria

The following criteria are applicable as follows:

- Positively eliminated 100%
- Reduced at least 75%
- Reduced by 50%
- Reduced by 25% to 50%
- Slight effect (less than 25%)

6.2.2 Degree of Correction Risk Indicator

The degree of correction risk indicator will be reflected according to the correction criteria.

Correction Criteria	Correction Risk Indicator
• Positively eliminated 100%	Very Low
• Reduced by 75%	Low
• Reduced by 50%	Medium
• Reduced by 25% to 50%	High
• Slight effect (Less than 25%)	Very High

Correction Risk Rating

It is important that every risk indicator must have a risk rating in order to come to a positive rating of the risk problem.

Correction Risk Indicator	Correction Risk Rating
Very Low	1.00
Low	0.75
Medium	0.50
High	0.25
Very high	0.0

It is now necessary to combine the degree of correction concept aspects in table form as illustrated in table 6.2.

Table 6.2: Combined illustration of the degree of correction aspects

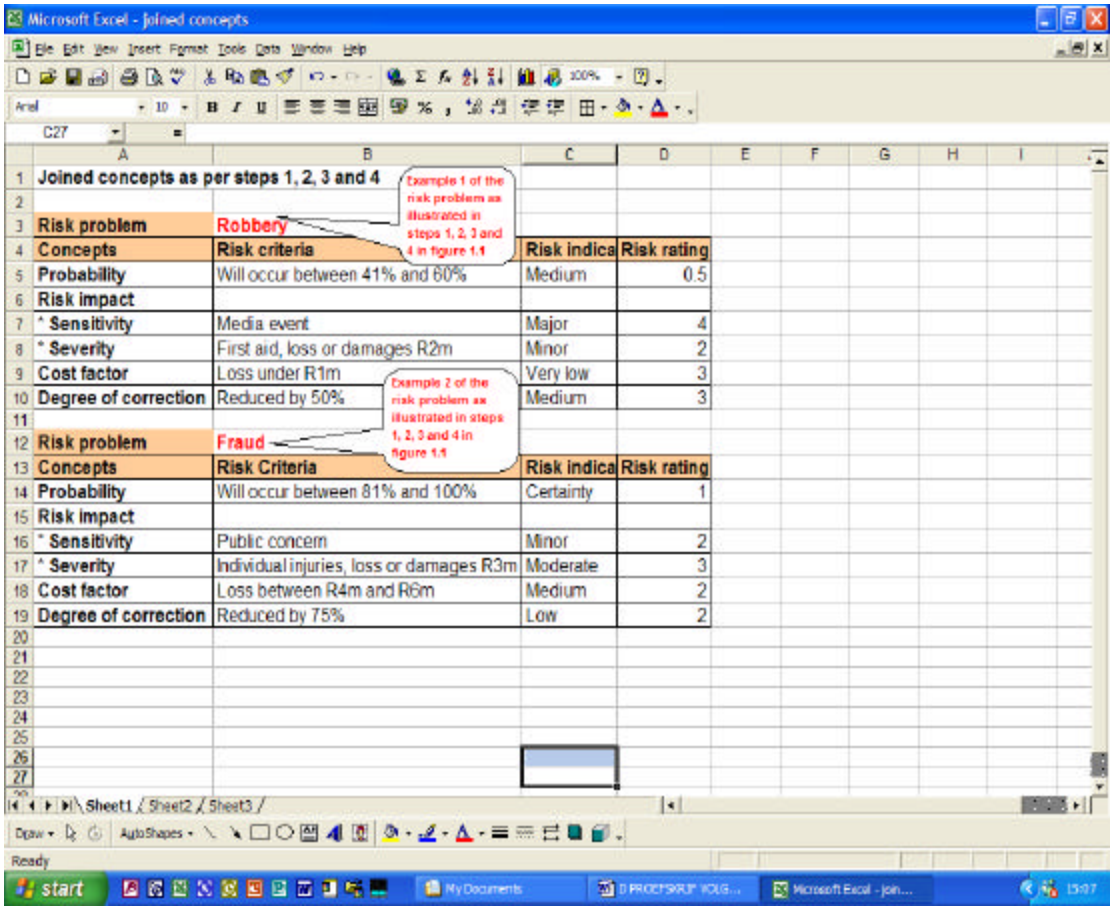
Risk Problem	Correction criteria	Correction Risk Indicator	Correction Risk Rating
Robbery	**Reduced by 50%**	**Medium**	**0.50**
Fraud	**Reduced by 75%**	**Low**	**0.75**

Source: Own compilation

6.3 JOINED CONCEPTS WITH THE DEGREE OF CORRECTION IN EXCEL FORMAT

The degree of correction concept as indicated in table 6.2. is joined with the other concepts (see tables 3.4, 4.3 and 5.3) in an Excel format as suggested in chapter one under point 1.6.3. The joining of these concepts will provide a better picture of the model appearance so far (see figure 6.1).

Figure 6.1: Joined concepts in Excel format



Source: Own compilation

6.4 CONCLUSION

From the above it should be noted that the degree of correction plays a vital role in the accurate outcome of the end result in the "TIQCAM" model. Secondly, there is a linear relationship between the degree of correction and the cost factor. The implementing of protection measures not only makes a difference on the cost of an organisation, but also ensures the mitigation of the risk.

The following chapter address the human factor concept, which is one of the concepts introduced by the researcher in rounding off the "TIQCAM" model.

CHAPTER 7

HUMAN FACTOR AS A CONCEPT IN QUANTITATIVE RISK ANALYSIS

7.1 INTRODUCTION

This discussion is the initiative of the researcher and is fundamental in combining all quantitative risk analysis concepts together.

The human factor, also known as the "CHHP" approach, [25] is the first concept, which will round the model off in an effective measuring way. The model which is developed (see point 7.4) for the quantifying of physical risks will create not only a more meaningful understanding, but will provide the decision maker with a more effective tool in managing risks.

It is often said that risks occur due to the fact that people don't know what they are doing. According to Bedell (1998:22) it is a definite risk not to know how to handle situations. Taking this statement into consideration it is thus the researcher's view that to analyse risks and to come to a reasonable conclusion, it is necessary to consider the important human factors.

---

[25] *"CHHP" approach is the researchers own design and takes human aspects such as, control measures, handling of risks, human attitude regarding risks and the organization procedures, in consideration*

This chapter will not only focus on the human factors, but will conclude the discussion on joining all the concepts as per chapters 3-6. The end result will also present the outcome of the "TIQCAM" model by involving the total risk rating, risk classifications and future actions (see figure's 7.2 and 7.3). Guidelines for the implementation of the "TIQCAM" model will conclude this discussion.

7.2 PERSPECTIVE ON HUMAN FACTORS

Human factor analysis and tests can be traced to the early efforts of engineers and psychologists and focuses on the systematically identification and evaluation of human errors[26] (Sawyer & Lowery 1994:1). According to Baybutt (1996:5), it is generally believed that 50 – 90% of business incidents can be attributed to human errors. There are various ways, of classifying human errors according to Baybutt (1996:7) The simplest is by (i) **omission error** – action not performed (ii) **commission error** – action is performed incorrectly and (iii) **extraneous act** - non-required action is performed instead of or in addition to required act.

According to Davies (2004:3) qualitative data plays a vital role in the human factor analysis and are sources of information in their own right. Data are important for two reasons, firstly, details of human errors, intensions, expectations, beliefs, and motives can only be accessed through natural personal accounts (discourse). Secondly, whilst the meaning of what people say is usually seen as inherent in the words they use (i.e. the meaning is semantic; thus leading to a simplistic distinction between accounts which are "true" and "lies") an approach via functional attribution theory sees all accounts as primarily functional (Davies 2004:3).

Researchers in the field of Human factor analysis, such as Davies (2004:3) Sawyer & Lowery (1994:1) and Baybutt (1996: 5), solely focus on the reliability of human factors and not in the complete combining of all relevant concepts (i.e. probability, impact, cost of risk, etc.) in a quantifiable manner.

Taking the foresaid views in consideration, it is the perception of the researcher that the human factor concept cannot be seen in isolation and should accommodate all other concepts (see chapters 3 – 6) in the quantitative risk analysis process.

The following discussion regarding the "CHHP" approach is specially developed to accommodate the human factor concept in quantifying risks in conjunction with concepts such as probability, impact, cost of risk and degree of correction, to ensure a reasonable accurate risk rating score.

7.3 HUMAN FACTOR LINK WITH THE "CHHP" APPROACH

As mentioned in footnote 25, the "CHHP" approach involves human factors such as (i) control measures, (ii) human attitude, (iii) handling of risk, (iv) policies and procedures. The "CHHP" approaches is not only focussing on humans per se, but also taking the overall measures of determining the probability of crime into account. According to McGoey (1990:6) quantitative analysis involves a decision making process for processing crime statistics involving aspects such as premises, location and history. The question under control measures (see 7.3.1) is design for the purpose to include the history, location and the industry.

7.3.1 Control Measures[27]

In most instances when risks are identified, it happens that there is a lack of control measures. This can be seen as a human task in assuring that control measures are in place to minimize identified risks.

The question for establishing the rating is as follows:

Q = Are you satisfied with the security control measures and the equipment used in preventing the risk?

---

[26] *Human error is any action that exceeds some limit of acceptability or performance for a process or system in which the human is a component (Baybutt 1996:7)*

[27] *For the purpose of this study, control measures will also includes equipment used in preventing risks.*

The answer in establishing the risk score is as follows:

The score is rated on a scale from 1-4 with 1 being the lowest ratio, which means that a satisfactory score is obtained. The highest score is 4, which means that no control measures and equipment are in place or in use and is therefore unsatisfactory.

7.3.2 Human aspect[28]

Human attitude towards the risk is of utmost importance, especially when confronted with criminal risks. For example, when a bank robbery occurs, what should the cashier's attitude towards the potential robber be? If it is one of negativity, it could place the lives of all bank personnel and visitors in great danger.

The question for establishing the rating is as follows:

Q = Are you satisfied with the attitude of personnel regarding the risk?

The answer in establishing the risk score is as follows:

The score is rated on a scale of 1-4 with 1 being the lowest ratio which means a satisfactory score is obtained. The highest score is 4, which indicates that the attitude aspect can be of a very risky nature for individuals and is thus unsatisfactory.

7.3.3 Handling of risks

The researcher experienced that the greatest problem in organizations and even in the security industry, is that individuals don't know how to handle risks. This can be ascribed to a lack in knowledge and skills.

---

[28] *The term "human" refers to decision makers, which could include personnel and management depending on the involvement in the risk situation.*

The question for establishing the rating is as follows:

Q = Are you satisfied that personnel have the necessary knowledge and skills in handling risk?

The answer in establishing the risk score is as follows:

The score is rated on a scale of 1-4 with 1 being the lowest ratio which means a satisfactory score is obtained. The highest is 4, which indicates that no knowledge or skills can have a tremendous impact on the organization in the event of managing risks and is rated as unsatisfactory.

7.3.4 Policies and procedures

It is of utmost importance that policies and procedures are put in place in managing risks within an organization. This is a management function and should be delegated or channelled down to personnel at floor level. According to Baybutt (1996:7) personnel should acquaint themselves with company written an unwritten policies and procedures, rules as well as computer software. Human errors in this regard can lead to increased risk situations.

The question for establishing the rating is as follows:

Q = Are you satisfied that company policies and procedures are in place regarding company risks and are you acquainted therewith?

The answer in establishing the risk score is as follows:

The score is rated on a scale of 1-4 with 1 being the lowest ratio which means a satisfactory score is obtained. The highest score is 4, which indicates that no policies and procedures are available in managing risks with a company is rated as unsatisfactory.

7.3.5 Combining human factors into a risk matrix

In discussing the abovementioned "CHHP" approach it is therefore necessary to combine the factors in order to establish a total point, which will then be quantified to a total point and integrated with all the other previously discussed concepts. A sample of such combination is shown in table 7.1.

Table 7.1: "CHHP" Approach Risk Matrix

Factor	Question	Score 1	2	3	4
Control Measures	Are you satisfied with the control measures and equipment used in preventing risks?			x	
Human Aspects	Are you satisfied with the attitude of the personnel regarding the risk?			x	
Handling of risks	Are you satisfied that personnel have the necessary knowledge and skills in handling risks?			x	
Policies and procedures	Are you satisfied that policies and procedures are in place regarding company risks?			x	
	Total Score				**11**

Source: Own compilation

7.4 HUMAN FACTOR CONCEPT IN THE DEVELOPMENT OF THE "TIQCAM" MODEL

With reference to point 7.2, the human factor also known as the “CHHP” approach, and contains questions in which a score is granted as indicated in the discussion below:

7.4.1 Control measures

Are you satisfied with the security control measures and the equipment used in preventing the risk?

Satisfied = 1

Unsatisfied = 4

7.4.2 Handling of risks

Are you satisfied with personnel having the necessary knowledge and skills in handling risks?

Satisfied = 1

Unsatisfied = 4

7.4.3 Humanity

Are you satisfied with the attitude of personnel regarding the risk?

Satisfied = 1

Unsatisfied = 4

7.4.4 Policies and procedures

Are you satisfied that company policies and procedures are in place regarding company risks and are you acquainted therewith?

Satisfied = 1

Unsatisfied = 4

Before the criteria, risk indicator and risk rating are discussed; it is necessary to consider all the aforesaid factors to establish the total score.

Scores are allocated to the different human factors and rated on a scale of 1-4, which means that 1 is the lowest score and can thus be accepted as

satisfactory. Therefore the highest score is 4, which indicates that immediate attention is needed to rectify the situation.

All the human factor's maximum scores (4) are taken into consideration to establish the total score (see table 7.1). The total score of 16 (4 questions x 4 maximum score) would indicate an unsatisfactory score whereas 1 is considered as the minimum score and an indication of a satisfactory indicator.

Human factor criteria

The following criteria are established by reverting the "CHHP" ratings into criteria scores as indicated below:

- Unsatisfactory score between 10-16
- Satisfactory to a unsatisfactory score between 4 - 9
- Satisfactory score between 1-3

Human factor risk indicator

The human factor risk indicator will be reflected according to the aforesaid criteria.

Criteria	Risk Indicator
• Score between 10 - 16	High priority attention needed
• Score between 4 - 9	Medium attention needed
• Score between 1-3	Adequate
• Score less than 3	No attention needed

Human factor risk rating

It is important that every risk indicator must have a risk rating in order to come to a positive rating of the risk problem. To establish the correct score, the total of 16 was divided into suitable scores for each indicator.

Human factor risk indicator	Human factor risk rating
High priority attention needed	9
Medium priority attention needed	5
No attention needed	2

It is now necessary to combine the human factor concept aspects in table form as illustrated in table 7.2.

Table 7.2: Combined illustration of the human factors

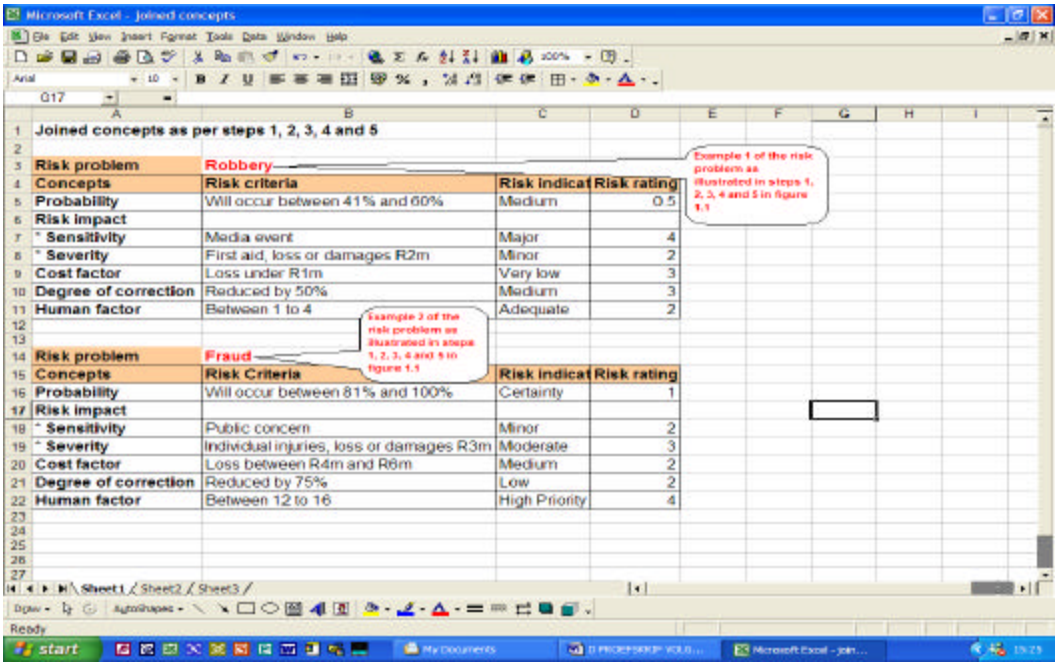
Risk Problem	Human factor criteria	Human factor risk indicator	Human factor risk rating
Robbery	Between 1-3	No attention needed	2
Fraud	Between 10-16	High priority attention needed	9

Source: Own Compilation

7.5 JOINED CONCEPTS IN EXCEL FORMAT

It is important that the concepts as per figures 4.1, 5.1 and 6.1 now be illustrated in Excel spreadsheet format as suggested in Chapter 1 under point 1.6.3. These aforesaid concepts are joined together in order to give the reader a better picture of the model appearance as per figure 7.1.

Figure 7.1: Joined concepts in Excel format



Source: Own compilation

7.5.1 Fundamentals of the "TIQCAM" theory

Referring to figure 7.1, the next phases play a fundamental role in the end result of the model, namely:

- Total Risk Rating;
- Risk Classification;
- Future Actions.

Bearing in mind that after discussing the aforesaid aspects, it will also form part of the quantitative risk analysis concepts displayed in the Excel format as per table 7.2.

7.5.1.1 Formula for calculating risk classification

The following scientific statement describes the range in which the "Risk Total" can be classified (see table 7.3).

Table 7.3: Scientific formula describing how the risk total can be classified

```
=IF(V4>=132,"VERY HIGH RISK",IF(V4>=99,"HIGH
RISK",IF(V4>=66,"SUBSTANTIAL RISK",IF(V4>=33,
"LOW RISK",IF(V4>=0,"MINIMAL RISK","NO
DATA")))))
```

Source: Own Compilation

Taking the abovementioned formula into consideration, it reflects equalization of the minimum and maximum risks.

- The lowest score will equal "0" when calculated against the minimum risk criteria.
- The highest score will equal "198" when calculated against the maximum risk criteria.

Taking the aforesaid scientific statement in mind, the universal formula for calculating the "risk total" is seen in table 7.4.

Table 7.4: Equation – Risk Formula

Risk Subtotal = Probability x (Severity + Sensitivity) x Cost x Human Factors Degree of Correction = Risk Subtotal – (degree of correction x risk subtotal) Risk Total = Risk Subtotal – Degree of Correction

Source: Own compilation

When substituting the abovementioned formula with the maximum and minimum risk ratings, the overall range within the respective risk ratings will then be "0" and "198" as classified in the aforesaid discussion. The following calculation is applicable in obtaining the different risk classification, for example:

Risk Subtotal = 1.0 x (5+5) x 5 x 4 = 200
Degree of Correction = 0.01 x 200 = 2
Risk Total = 800 – 8 = 198

The risk formula as indicated in table 7.4 consists of six risk concepts. For this reason the maximum risk total of 198 has been divided by the six concepts (198/6 = 33) to at least establish a risk rating range for the five different risk classifications as per table 7.5.

Table 7.5: Different Risk Classifications

Minimum	0 – 32
Low	33 – 65
Medium	66 – 98
High	99 – 131
Very High	132 - 198

Source: Own compilation

7.5.1.2 Total application of concept and risk rating in establishing the risk classification

This is the final stage in establishing the total outcome of the two examples namely, “robbery” and “fraud” risk classifications. It will thus indicate whether the two risks is a minimum or very high risk in the magazine distributing company.

- Calculation formula for the “robbery” risk

  Probability 0.5 x (Sensitivity 4 + Severity 2) x Cost Factor 3 x Human Factor 2 = Risk Subtotal 18
  Degree of Correction 0.50 x Risk Subtotal 18 = 9

  Risk Subtotal 18 – Degree of Correction 9 = Risk Total 9

  Risk total of 9 indicates a minimum risk as indicated in table 7.5

- Calculation formula for the “Fraud” risk

  Probability 1 x (Sensitivity 2 + Severity 3) x Cost Factor 2 x Human Factor 4 = Risk Subtotal 40

  Degree of Correction 0.75 x Risk Subtotal 40 = 30

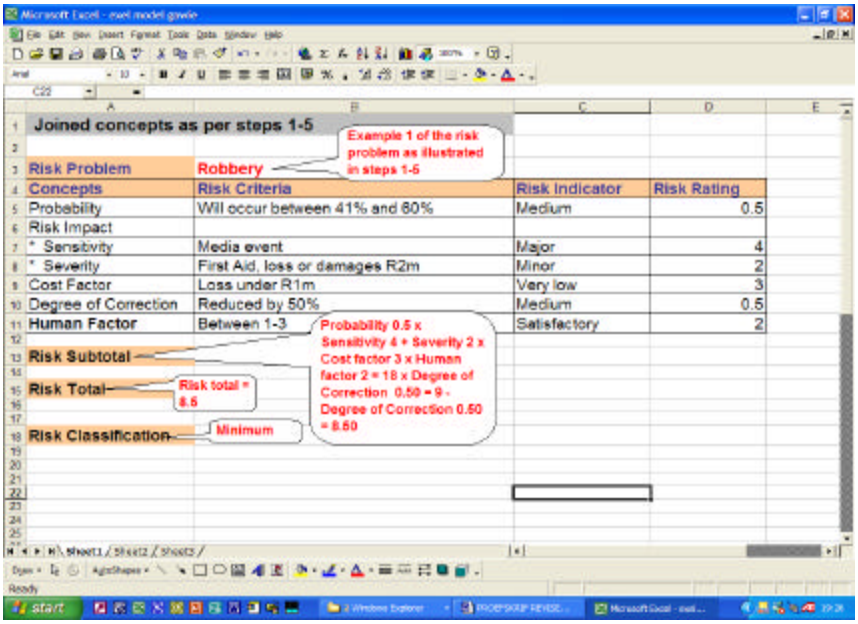
  Risk subtotal 40 – Degree of Correction 30 = Risk total 10

  Risk total of 10 indicates a minimum risk as indicated in table 7.5

Taking the aforementioned two examples into consideration, it now reaches the stage where the calculation formula is joined with the already established concepts as mentioned in table 7.2.

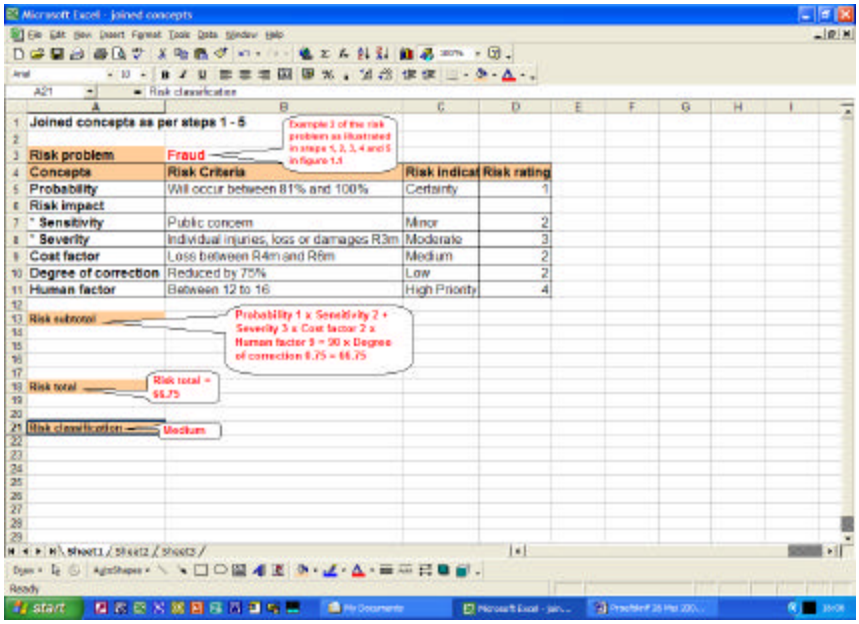
The risk subtotal, risk total and the risk classification are displayed in figure 7.2 and 7.3 below:

Figure 7.2: Joined calculation of the robbery example



Source: Own compilation

Figure 7.3: Joined calculation of the fraud example



Source: Own compilation

From the above figures it is clear that the "TIQCAM" model quantifies the risks in a manner that any management can secure the effective-ness in managing their own risks.

7.6 GUIDELINES FOR THE IMPLEMENTATION OF THE "TIQCAM" MODEL

The "TIQCAM" model can be implemented by using it not only in the private security industry, but also in all business sectors where physical risk is applicable. The "TIQCAM" model can also form part of any business policy where there can be worked from and it is thus suggested that the implementation takes place in phases as discussed in sub-section 7.5.1.

7.6.1 Phases for implementing the "TIQCAM" model

The researcher is of the opinion that the private security industry should have a policy whereby security managers must be knowledgeable in the use of the "TIQCAM" model to analyze physical risk. From this point of view the following phases are suggested.

Phase 1: Approval by principle

The implementation of the “TIQCAM” model for training purposes should be approved by principle so that security managers can be aware of the existence of the quantitative risk analysis model. This should minimize the stigma of inferiority that security managers are only knowledgeable in the security aspects and not in the specialized field of risk analysis. Naseb security is the first to grant approval that all their security managers be trained in the analyzing of physical risk, which can form part of their tendering policy for new business and is thus also in line with corporate governance which places the emphasis strongly on the risk analysis aspect (See Chapter 2 point 2.6).

Phase 2: Issuer of Policy

The policy-making component must give the necessary assistance to the quantitative risk analysis model ("TIQCAM") and it should be in writing as soon as possible. This will enable the quick implementation of the model.

During a Naseb security[29] director's meeting held on 3 February 2004, it was suggested that Naseb should draft a policy which will enable them to make use of the "TIQCAM" model, not only for their own purposes, but also for use in identify their clients' risk. A concept draft will be discussed at a next board meeting, which will take place in August 2004.

Phase 3: Marketing of the "TIQCAM" model

When the policy framework is in position, then the "TIQCAM" model can be introduced as a cost-effective approach in corporate training, not only for security managers but also managers in their different fields of interest.

Phase 4: Training of security managers

The researcher is of the opinion that training is one of the most effective ways in implementing models. Security managers need guidance in the use of the "TIQCAM" model as part of management training. The initial formal training is a direct outcome of this research. The researcher trained his security managers in the use of the aforesaid model and in general no problems were experienced. Symposiums and risk management conferences are still the best form of promoting the "TIQCAM" model as a practical training method for security managers**.**

[29] *Naseb security originate in 1999 due to an out sourcing process at Naspers, whereby the researcher and two partners started the company called "Soloprop 1049 t/a Naseb (See out sourcing and approval letter from Naspers - Appendix E & F).*

7.6.2 Implementation and management of the "TIQCAM" model

The implementation of the "TIQCAM" model starts during the identification process, which is the beginning of the training approach that should take place. Security managers that are involved in the analyzing of risk should be thoroughly trained and informed how to undertake the task, especially in the use of the aforesaid model. The training of managers will probably take place during normal working hours, because of the fact that the whole process of risk analysis forms part of the work situation. Due to the fact that security managers are in need of guidance in the use of the "TIQCAM" model, arrangements should be made for a learning programme, as discussed in the following sub-section 7.5.3.

7.6.3 Guidance for the training of security managers in the "TIQCAM" model

The researcher foresees that the training of security managers in the use of the "TIQCAM" model will rather take place on a modular basis than a self study package as this training is more of an on-the-job training orientation.

Each of the "TIQCAM" model concepts will form a training module. This will enable the student and/or security manager not only to understand the process of quantitative risk analysis, but also the important role that the concepts play in the end result of the correct classifying of risks within an organization. With the researcher's training of Naseb security managers, the same basis was followed and it and was successfully implemented. The training approach followed by the researcher involved the following steps:

- Orientation of the "TIQCAM" model as discussed in Chapter 2;
- Fundamental concept approach as discussed in Chapters 3, to 6
- The need for the private security manager to be trained in the quantitative risk analysis model as discussed in Chapter 7.

With the aforesaid approach in mind, it may happen that in future this "TIQCAM" package can be registered as a training package, which can be used by all security training institutions in South Africa or internationally.

7.7 CONCLUSION

It is the researcher's contention that the security industry is in urgent need of a quantitative analysis measuring tool, such as the "TIQCAM" model, in securing better skilled and knowledgeable managers able to identify and manage risks.

It is also said that security managers have to remember that they cannot be lax in security by just patching what they think is wrong. A better understanding of the risk analysis process will enable them to conduct a risk reduction analysis and to advise their clients on various options to secure their assets.
With the development of the "TIQCAM" model as an Excel measuring tool, it will not only secure value-added services, but will also form the basis from where the security manager can follow a structural process in the total risk concept use. The enclosure of the different risk concept approaches implies that a more effective, realistic and useful assumption can be obtained of how high or low risks are in companies.

It was also stated that with the implementation of the 'TIQCAM" model as a measuring tool, it could also secure a policy-making role within organizational context.

The implementation of the aforesaid model is also described by means of the model and presented in phases for implementation. Seeing that these phases play a fundamental role in the implementation, the emphasis is strongly placed on the "training" phase, which is the phase that is the most effective medium to secure implementation of any model. From the aforementioned discussion, the following chapter will round off the whole research project by looking at the findings and recommendations regarding the "TIQCAM" model.

CHAPTER 8

FINDINGS AND RECOMMENDATIONS

8.1 INTRODUCTION

With the non-existence of a suitable physical quantitative risk analysis model for the private security industry , this research project was focused on the development of an effective and/or useful measuring tool for the South African security manager. The first model called “FAMASER” is taken as the basis where upon an easy-to-use model, as requested by security managers, (see point 1.6.3) is developed. This model called the Total integrated quantitative concept analysis model (“TIQCAM”), were received with great enthusiasm by security delegates during the pre-testing of the model (see point 1.5.3.4), which in their views, is a breakthrough for the private security industry in South Africa.

This research also sets the necessary guidelines, which are fundamental in the measuring of risks to ensure a realistic outcome of the risk classification by applying workable concepts. The applications of these concepts are far-reaching, and any dynamic system that meets the assumptions can be analysed by the “TIQCAM“ approach.

This chapter intends to establish whether the goals are achieved regarding the overall research done in this thesis, and to come up with findings relating to the following:

- Objectives;
- Hypotheses;
- Methodology;
- Empirical data.

Recommendations and possible future research regarding the possibility of extending or developing an advanced quantitative risk analysis model will end this study.

8.2 FINDINGS

8.2.1 Findings relating to the objectives

With reference to Chapter 1 under point 1.3, regarding the research objectives, the need for a quantitative risk analysis model in the private security industry has been determined by means of personal interviews and using an information schedule (see point 1.5.3.3). It was determined that security managers do not receive formal training in quantitative risk analysis and that no suitable models exist that can be used as a software tool in analysing their clients' risks as a value-added service.

A theoretical investigation also indicates that although a quantitative analysis model on decision-making exists (see point 1.2 - referring to C.J.Roelofse), the "TIQCAM"[30] model especially intends to provide an Excel software tool for the private security industry in South Africa. A pre-test (see point 1.5.3.4) was done where security managers expressed the need for a so-called "Easy-To-Use" model.

During a presentation of the 'TIQCAM' model to a group of security managers, the members reacted positively to the model and they see it as a great breakthrough for the security industry. The conclusion is therefore that there is a definite need for a quantitative risk analysis model that can be used in a scientifically justifiable way by the security industry.

8.2.2 Findings relating to the hypothesis

By taking the abovementioned finding on the objectives into consideration, it is clear that this supports empirically the hypothesis set in Chapter 1, paragraph 1.4.

[30] *The "TIQCAM" model originate from the first developed model called "FAMASER" (See discussion under point 1.5.3.4).*

With reference to the information schedule (see appendix A) it is clear that both the hypothesis (see point 1.4) supports the view that no quantitative risk analysis model exists or that security managers in the researcher's survey (see Table 1.2) are knowledgeable in all the aspects of quantitative risk analysis.

Based on these facts it can be assumed that no practical quantitative risk analysis model exists for the South African private security industry and that security managers are unskilled in this regard, gave rise to a theoretical model to quantitatively measure risks by integrating all the necessary risk analysis concepts, this includes the newly established concept by the researcher (see Chapter 7 – Human factor link with the "CHHP" approach). This proves the integrated nature of the "TIQCAM " model and that the practical use can be a value-added tool in the hands of the security manager.

8.2.3 Findings relating to the methodology

Each researcher has his own way of approaching his subject and the formulation thereof. For the researcher, the methodology that was followed was not only satisfactory, but also gave rise to certain deductions with regard to the development of a quantitative risk analysis model for the security industry.

The methodology in this study strengthens this deduction in the following ways:

- In the security industry, the development of a quantitative risk analysis model is a strategy that can be followed for human resource development. In the light of the strong emphasis placed on risk analysis in South Africa (King, section 2.6, p.68), risk analysis should form one of the cornerstones of successful training of security managers.

- The application or use of a risk analysis model can only be communicated by means of an expert instructor. Printed material will still form the basis

of the learning material, as it remains the most viable medium to represent quantitative aspects regarding the presentation of a model.

- A quantitative risk analysis cannot be implemented effectively without the support of the policy makers. Consequently, there has to be a training policy that addresses the specific application of a physical risk analysis model by security managers. It not only creates a favourable marketing opportunity, but also the possibility for the private security industry to ensure an added value to service for their clients.

- Quantitative risk analysis is no longer isolated from the total spectrum of physical security services, but rather forms an integral part of the total security strategy.

8.2.4 Findings relating to the empirical data

Coetzee exclaims in Roelofse (2001:22) “Laat empirie nou spreek tot teorie” (Let the empirical now speak to theory). It is the researcher’s perception that empirical data can only strengthen the theory especially where model development is applicable.

In this study a new theoretical model has been proposed and empirically tested in Chapters 3 to 7. The formulas for calculating the risk classification (see tables 7.3, 7.4 and 7.5) involved the different risk analysis concepts, has their own risk criteria, risk indicator and risk rating.

Although all the concept formulas are multiplied with each other, the only subtract able concept is the “ the degree of correction” (see Chapter 6), which focuses on subtracting the security measures that are in place. Calculations are presented in percentage, which not only makes the “TIQCAM” model more reliable, but also enables the model to be more accurate in the outcome of the risk classification.

When joining all these concepts together, it forms a suitable empirical software tool, which can be useful in any decision-making process.

8.3 RECOMMENDATIONS

Before any recommendations can be made it is necessary to first look at the following two very important aspects:

- Possible value of this research;
- Possible shortcomings of this research.

Possible value of this research

This research with regard to a risk analysis model for the security industry in South Africa has established that a need exists to develop a quantitative risk analysis model that serves as a handy tool in the application of physical risks. What makes this model unique is the fact that an integrated approach was followed in the application of different risk concepts to ensure an accurate and effective result during the risk analysis process. This concept approach is also a first for the security industry where the human factor, as one of the most important concepts, has not been excluded from the total risk analysis process. A training curriculum that can be used in human resource development is also currently under consideration. In this way, the security industry's aim to ensure a total and effective security service to clients at all times can be strengthened. This model also creates the possibility for the development of a more advanced quantitative risk analysis model.

As this research focuses on the security manager as an entity, it is possible that the model can also be utilised by security commanders and/or shift leaders. Therefore, this research also has possibilities for application outside the security milieu.

Possible shortcomings of this research

A big restrictive factor is the availability of funds to create the necessary infrastructure to establish a risk analysis training system that uses quantitative risk

analysis methods to strengthen security management in South Africa's knowledge and skills level. The real cost-effectiveness of human resource development in quantitative risk analysis has also not been determined in the course of this research.

8.3.1 Recommendations for the industry

An awareness campaign must be undertaken by means of interviews and briefings to all senior top management members regarding the value and practical implementation of the "TIQCAM" model for the security industry. The research suggests that this takes place in phases as expounded in Chapter 7, section 7.5.1, that includes some of the following:

- Obtaining approval in principle for the training of security managers regarding the "TIQCAM" model within the security industry.

- Promulgating policy by the policy makers within the security industry so that learning opportunities are created for the security manager.

- Training of security managers to not only increase the level of knowledge regarding risk analysis, but also to be of greater value to their clients. This addresses the added value to service concept.

- Marketing of the model will also make the top security management aware of what the model entails and what possibilities it has.

8.3.2 Recommendations for further research

Quantitative risk analysis as a human resource development strategy in the security industry should be investigated continuously. The development of more advanced risk analysis models can also lead to a more specialised task for individuals within the occupational milieu.

8.4 END

A quantitative risk analysis model for the security industry is an unfamiliar phenomenon, firstly due to their lack of involvement in risk analysis and ignorance of the subject, and secondly due to their continued focus on the physical aspect of security (e.g. entrance control, escorting, etc.). With the still growing security industry at national and international level, it is essential that security managers develop their knowledge and skills in the use of the correct aids to analyse the risks within their own industry and in that of their clients. The value of the quantitative risk analysis model ("TIQCAM") can be considered as a training strategy to strengthen the levels of knowledge and skills of all security managers.

BIBLIOGRAPHY

Addison, S. 2002. Introduction to security risk analysis and the cobra approach. C & A security system report (Online serial). Available : www.security-risk-analysis.com

Apostol, T.M. 1969. A short history of probability (Online serial). Available. www.cc.gatech.edu

Babbie, E. 1992. The practice of social research (6th edition). Belmont, CA : Wadsworth

Bailey, K.D. 1987. Methods of social research (3rd edition). New York: Collier Macmillan Canada, Inc.

Baybutt, P. 2003. Human factors in process safety and risk management : Needs for models, tools and techniques. Columbus, Ohio

Bedell, G. 1998. The king of capitalism. *Cosmoman*. November 1998

Berryman, P. 2002. Risk assessment : The basics. *Internal journal.* February 16, 2002

Blackburn, A. 2002. Product description (DBS Accord). Dorset (UK) : DBS publication

Blackburn, A. 2003. Product description - risk assessment. Dorset (UK) : Published report by DBS Financial Systems

Bosch, J.G.S. 1999. The role of structure of the private security industry in South Africa. *ISSUP Bulletin*. Pretoria

Broder, J.F. 2000. Risk analysis and the security survey. Second edition. Boston: Butterworth-Heinemann

Christman, J.H. (a) 2003. History of Private Security, Part 2. (online serial). Available. www.iapsc.org/publication www.iapsc.org/publication

Company Act and Regulations, Act 61 of 1973

Contractors regulations as per government notice 25207 of 2003

Davies, J. 2004. What's in a number? Quantitative approaches to human reliability assessment. *Workshop presentation.* 27 April 2004.

Davis, L. 2002. Risk assessment. All hands consulting services . South Carolina.

De Vos, A.S. (ed) 2002. Research at grass roots. Pretoria : Van Schaiks publishers

Dempster, C. 2002. Crime wave feeds SA security boom. (Online serial). Available. www.news.bbc.co.uk

Du Plooy, G.M. 2001. Communication research : techniques, methods and applications. Cape Town: Juta & Kie

Du Preez, G.T. 1994. Professionalisering. Pretoria : UNISA

Eberlein, E. & Karsten, P. 1998. The generalized hyperbolic model : Financial derivatives and risk measures. *Working paper 56* . Univerity of Freiburg

Eksteen, L.C. 1997. Pharos major dictionary (14th edition). Cape Town : National book printers

Fine, W.T. 1997. Mathematical evaluations for controlling hazards. New York : University (Courant Institute) publication

Fischer, R.J. & Green, G. 1992. Introduction to security. Stoneham (USA) : Butterworth-Heinemann

Glazer, S. 2001. What is an empirical article?. (Online serial). Available. www.psych.sjsu.edu/sglazer

Glosser, G. 1999. Lessons on introduction to probability. (Online serial). Available. www.mathgoodies.com

Golafshani, N. 2003. The Qualitative report - Volume 8 Number 4. Toronto

Groenewald, J.P. 1988. Maatskaplike navorsing : ontwerp en ontleding. Pretoria : Human & Rousseau uitgewers

Hall, M. 2003. Private security guards are homeland's weak link. (Online serial). Available. www.usatoday.com/publication

Hassenzahl, D. M. (2002, March, 12). Risk analysis education philosophy (Online serial). Available : david.hassenzahl@ccmail.nevada.edu (2003, Nov.16)

Hayes, F. 2003. The excel addict. The online newsletter for risk analysis and spreadsheet forecasting. Available : www.crystalball.com

Hilton, A. 2002. Should qualitative and quantitative studies be triangulated? Cheshire.

Huysamen, G.K. 1994. Methodology for the social and behavioural sciences. Pretoria: Sigma Press

Irish, J. 1999. Policing for profit: the future of South Africa's Private Security Industry. *Monograph No 39*. Pretoria. August 1999

Jenkins, B.D. 1998. Security risk analysis and management. Published report. USA

Kastrup, U. (2000, April, 11) Risk/Interdependency modeling (Online serial). Available . kastrup@sipo.gess.ethz.ch (2003, Jun.8)

King, M.E. 1994. The King report on corporate governance. Published report. Parklands: Institute of Directors in Southern Africa

Koller, G. 2000. Risk modeling for determining value and decision making.Oklahoma : Chapman & Hall publication

Kruger, P. 2003. Opsomming van versekering vir Media24 Beperk. Versekeringsverslag September 2003

Le Roux, G.J. (a) 2002. Development of a security risk analysis model : the basics. *Nasap in-house publication*

Le Roux, G.J. (b) 2002. Security training career path. Artikels rondom die risikobeheerkomponent binne organisatoriese verband. Naspers : *Inhuis publikasie*

Le Roux, G.J. 2000. Die posisionering van risikobestuur binne Naspers. Unpublished MA dissertation. Pretoria : UNISA

Levey, J.S. & Greenhall, A. 1985. The Concise Columbia Encyclopedia. South Carolina : Columbia University Press

Marais, C.W. 2002. Safety and Security in South Africa 1999-2000. UNISA

Martin, P. K. & Tate, K. 2002. A step by step approach to risk assessment. Cincinnati OH.

Marx, S., Van Rooyen, D.C., Bosch, J.K. & Reynders, H.J.J. 1998. Ondernemingsbestuur. Tweede uitgawe. Pretoria : J.L.Van Schaik uitgewers

May, L. 1996. Managing catastrophe risk. (Online serial). Available. www.iso.com/studies

McGoey, C.E. 1990. Crime foreseeability. (Online serial). Available. www.crimedoctor.com

Mouton, J & Marais, H.C. 1991. Metodologie vir die geesteswetenskappe : basiese begrippe. Pretoria : Raad vir Geesteswetenskaplike Navorsing

Mun, J. 2002. Applied risk analysis: Moving beyond uncertainty (Online serial). Available. www.crystalball.com

National Key Point Act 102 of 1980

Neser, J.J., Joubert, S.J. & Sonnekus, E.F. 1995. Inleiding tot die metodologie. Studiegids vir KRM100-5, PNL100-C en POL100-H. Pretoria : Unisa

Neuman, W.L. 1997. Social research methods : quantitative and qualitative approaches. (3rd edition). Boston : Allyn & Bacon

Ozier, W. (a) 2003. Risk metrics needed for IT-Security. (Online serial). Available. www.theiia.org/publication

Ozier, W. (b) 2003. Introduction to information security and risk management. (Online serial). Available. www.theiia.org/publication

Padwa.H. 2001. What's wrong with the "Security" industry in the US. Boston. 17 September 2001

Patton, M.Q. 2002. Qualitative evaluation and research methods (3rd edition.). Thousand Oaks, CA: Sage Publications, Inc.

Private security industry regulatory authority (PSIRA), Act 56 of 2001

Reksnes, H.O. 2003. Risk communication-an important tool in risk analysis. *Norwegian food research Institute journal*. July, 2003

Render, B., Stair, R.M.(Jr.) & Hanna, M.E. 2003. Quantitative analysis for management. Upper Saddle River : Prentice Hall

Roelofse, C.J. 2001. The development and application of a quantitative decision-making model to determine cost-efficiency in the application of short-term crime prevention measures, using a quantified crime hypothesis. Unpublished Doctorate Thesis. Turfloop : University of the North

Rogers, F.C. 1997. Administration and management of security at local government level:towards a policy for safety and security. Unpublished MA dissertation. Pretoria: University of Pretoria

Sawyer, D. & Lowery, A. 1994. CDRH's role in promoting user-oriented design. *Medical journal (US)*

Schirick, E. 2000. Risk analysis and evaluation. *Camping magazine*. July, 2000

Schönteich, M. 2002. *Security.* South Africa Survey. 2001-2002. Pretoria

Schuyler, J. R. 2001. Risk and decision analysis in projects (2nd ed.). Pennsylvania: Project Management Institute, Inc.

Security Officers Act 92 of 1987. Government printer : Pretoria

Shaw, G. 2002. Effective security analysis. *IT-Security journal*. April, 2002

Shimonski, R.J. 2002. Risk assessment and threat identification.*Window security.* November 2002

Spencer, S. 1997. Private security. (Online serial). Available. web.archive.org/publication

Stamatelatos, M.G. 2000. Risk assessment and management, tools and applications. Safety presentation. NASA : USA

The security officers amendment Act 104 of 1997. Government printer : Pretoria

Valsamakis, A.C., Vivian, R.W. & Du Toit, G.S. 2000. Risk management. Second edition. Durban:Butterworths

Van der Westhuizen, J. 1989. Beveiligingstrategie in die privaatsektor - Berekening van aanvaarbare risikovlakke. *Acta Criminologica*. Volume 2 (1)

Van Vuuren, J.W.J. 1992. Beveiliging in die plaaslike owerheidsektor. Ongepubliseerde MA verhandeling. Pretoria : UNISA

Van Vuuren, J.W.J. 1998. The management of security in the new South Africa : is it working? *Servamus*. February, 1998

Wayne, L.W. & Albright, S.C. 1997. Practical management science : spreadsheet modeling and applications. Belmont : Wadsworth publishing

Weaver, B. 2003. How to minimise negligent hiring. (Online serial). Available. webmaster@zerofoundation.com

Wold, G.H. & Shriver, R.F. 1997. Risk analysis techniques. *Disaster recovery journal*. August, 1997

APPENDIX A: INFORMATION SCHEDULE FOR SECURITY MANAGERS

Question 1	Specific	Answer with X
How is "risk analysis" defined in your organization.	Quantification of uncertainty Quantitative estimation and analysis of potential problems Quantified cost initiatives Quantitative list of schedule and technical risks Probable cost estimate Sensitivity analyses Judgemental estimate of low-high range *Not really defined	

Question 2	Specific	Answer with X
Is "risk analysis" a separate task, or is it an integral part of the cost	Integrated Mixed Partially or always separate task *Not really defined	

Question 3	Specific	Answer with X
What computer tools are used to support risk analysis	In-House (Customized) Tools supplied by consultants *None	

Question 4	Specific	Answer with X
Is risk analysis considered to be a highly specialized skill.	Yes *No	

Question 5	Specific	Answer with X
To what degree is analysis, as defined here, accepted by management.	Unqualified acceptance Acceptance varies with the manager Yes, as long as very difficult issues not encompassed Slight to moderate acceptance *Accepted as information only. Managers in denial *Listen attentively then do as please *Not well accepted. " Can do" optimism prevails	

*** Negative rating**

Question 6	Specific	Answer with X
Is there a functional department	Auditors	

responsible for performing risk analysis.	Management *Not applicable *Not assigned specifically	

Question 7	Specific	Answer with X
Does your company provide internal training or class in risk analysis.	Yes, formal training Yes, external Only informally *None	

Question 8	Specific	Answer with X
As preformed by your organization, is risk analysis mostly judgemental or based on statistical projections from historical data.	Statistical analysis of history Low - High range picked without analysis Guided Survey *Not really defined	

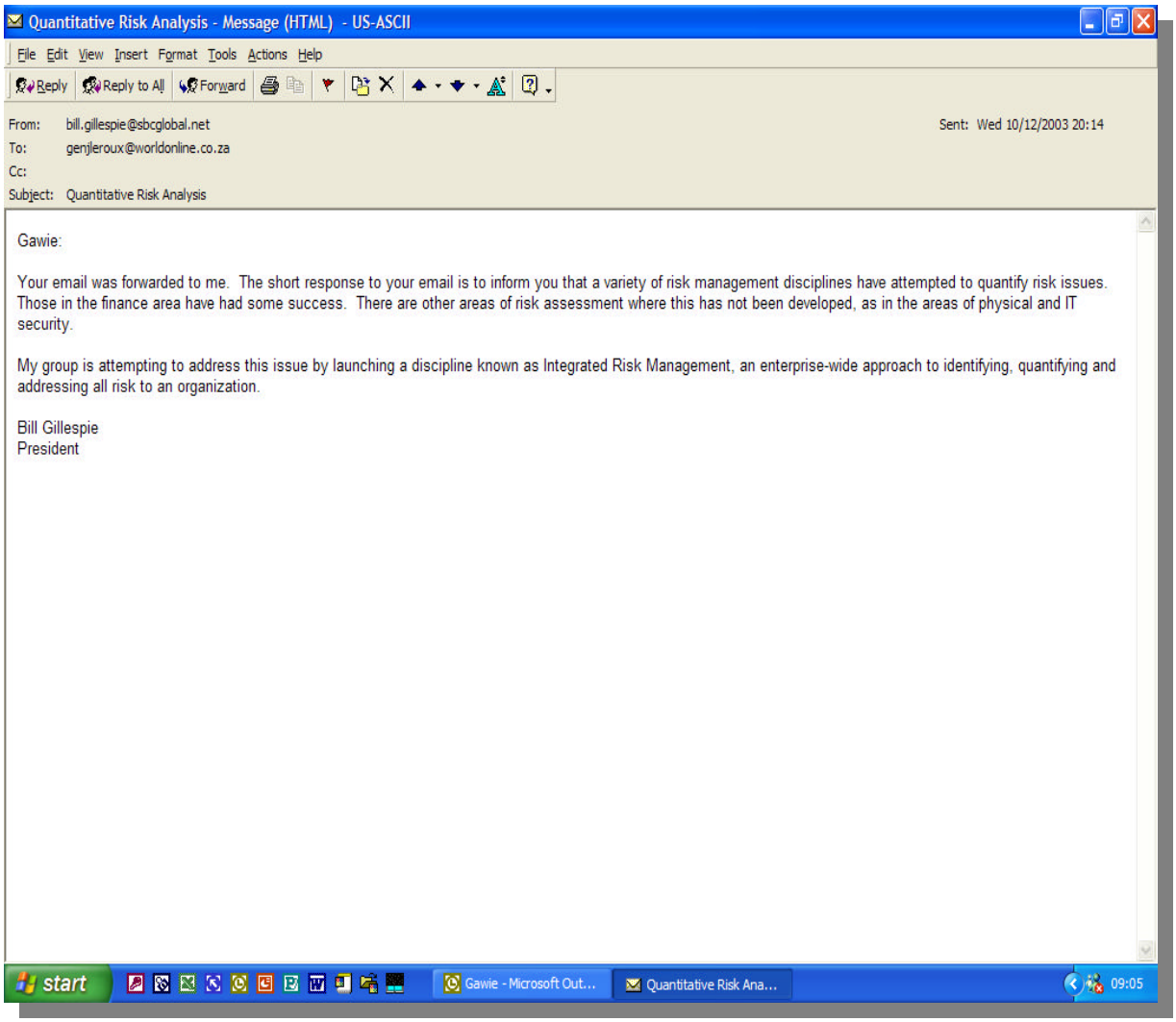
Question 9	Specific	Answer with X
How do you display the outcome of risk assessment to management or your clients.	Quantitative risk display Qualitative risk display *None	

Question 10	Specific	Answer with X
Analysts tend to prefer certain types of probability distributions. What distribution type does your organization find best	Normal *None / irrelevant	

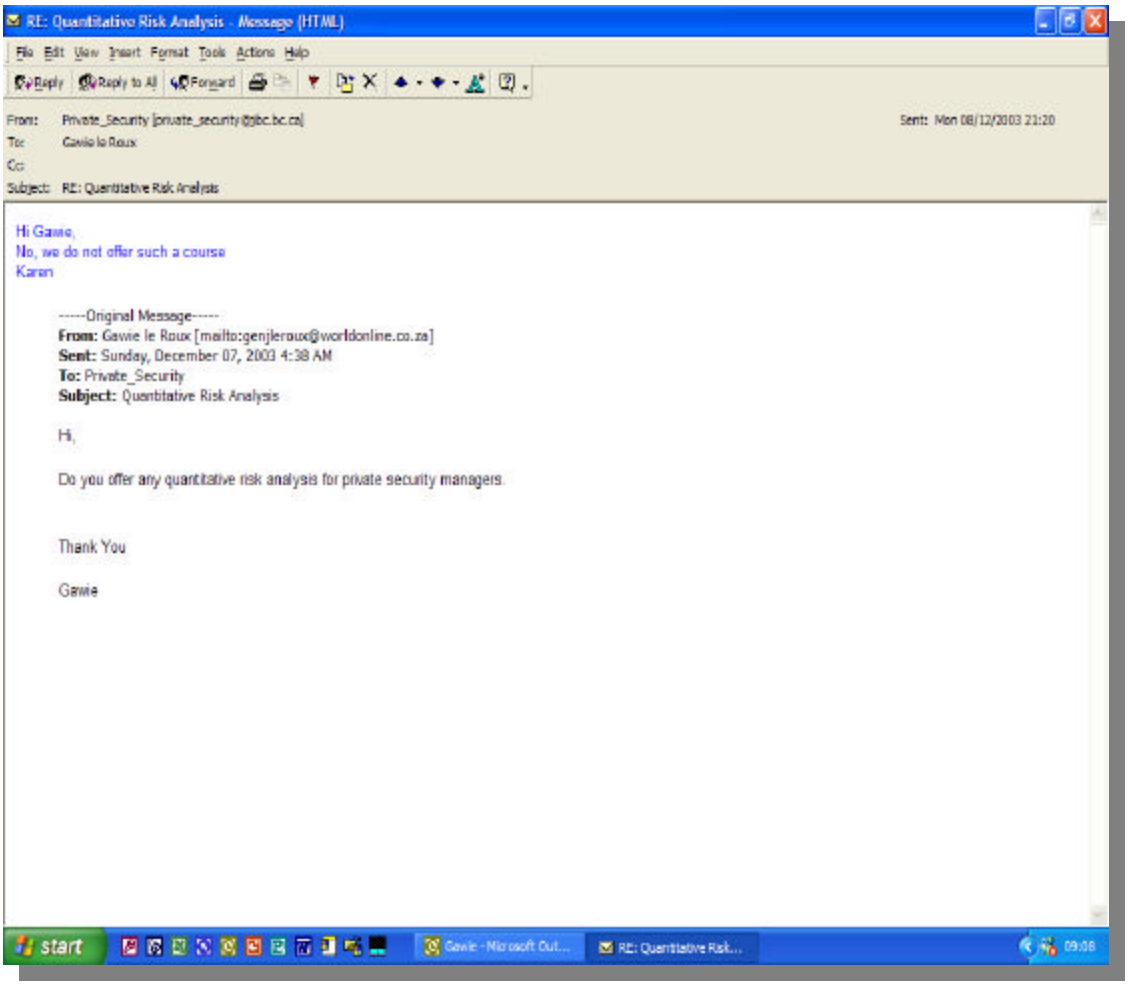
Question 11	Specific	Answer with X
When your organization finds unacceptably high risk, how do you reduce the risk.	Improve at higher cost Second opinion from a professional *Stop work and wait for affordable technology Look at various other risk management approaches Adjust the process *No idea	

Question 12	Specific	Answer with X
Do your company offer and or carry out risk analysis as part of your service to your clients.	Yes. Not using a risk analysis tool Yes, by contracting a risk analyst *No, form not part of our service to the client	

APPENDIX B: QUANTITATIVE RISK ANALYSIS E-MAIL MESSAGE NO 1



APPENDIX C: QUANTITATIVE RISK ANALYSIS E-MAIL MESSAGE NO 2



APPENDIX D: SECURITY SURVEY CHECKLIST

Security Survey Work Sheets

This is a basic guide that may be used to assist personnel in performing physical surveys in most industrial settings.

General Questions before Starting Survey

• Date of survey.
• Interview with [name of decision maker].
• Number of copies of survey desired by client, to be forwarded to:
• Obtain plot plan. Plot the production flow on plot plan and establish direction of north
• Position and title of persons interviewed.
• Correct name and address of plant.
• Type of business or manufacture.
• Square footage of production or manufacturing space.
• Property other than main facility to be surveyed is located at:
• Property known as:
• Property consists of:
• What activity is in progress here?
• Is there other local property that will not be surveyed? Why?
• If plot plan is not complete, sketch remainder of property to be surveyed.

Number of Employees

• Administrative—total number all shifts
• Skilled and unskilled—total number on each shift:
1st shift
2d shift
3d shift
Maintenance/clean-up crew
Normal shift schedule and break times
• Salaried
1st shift
2d shift
3d shift
Maintenance/clean-up crew
• What days of the week is manufacturing in process?
• Are employees authorized to leave plant during breaks?
• Are hourly employees union or not?
• Are company guards in union bargaining unit?

Cafeteria

• Where is cafeteria located?
• What are hours of operation?
• Is it company or concession operated?
• What is security of proceeds from sales?
• What is security of foodstuffs?
• What is method of supply of foodstuffs?
• How are garbage and trash removed?
• Where is location of vending machines?

• Where is change maker/ if any?

Credit Union

• Where is credit union located?
• How is money secured?
• How are records secured?
• How is office secured?
• What are hours of operation?
• How much money is kept during day and overnight?

Custodial Service

• Is it outside contract or company employees?
• What hours do they actually start and complete work?
• Do they have keys in their possession?
• How is trash removed by them?
• Who, if anyone/ controls removal?
• Who controls their entrance and exit?
• Are they supervised toy any company employee?

Company Store

• Where is company store located?
• What are hours of operation?
• What method is used to control stock?
• How is stock supplied from plant?
• Number of clerks working in store?
• How is cash handled?
• When are and who performs inventories?
• How are proceeds from sales secured?
• How is the store secured?

Petty Cash or Funds on Hand

• In what office are funds kept?
• What is the normal amount?
• How are these funds secured?

• Who has general knowledge of amount normally on hand?

Classified Operations

• Is government classified work performed?
• What is the degree of classification?
• How are classified documents secured?
• What is security during manufacture?
• What is classification of finished product?
• Are government cognizant officers on premises?
• Is company classified R&D performed?
• Is company classified work sensitive to industry?
• What degree of security is it given?
• What degree of security does it require?
• What are the locations of the various processing areas and

containers?

Theft Experience

• Office machines or records.
• Locker room incidents.
• Pilferage of employees' autos.
• Pilferage of vending machines.
• Pilferage from money changer.
• Thefts of company-owned safety equipment.
• Theft of tools.
• Theft of raw material and finished product.
• Are thefts systematic or casual?
• Have any definite patterns been established?
• Are background investigations conducted prior to employment of any personnel?
• What category of personnel is investigated?
• What is the extent of investigations?

The foregoing questions/ answered properly/ will assist you in developing the degree of control required for various areas/ information that can be secured only through an interview—the more probing the better. You should now also have a working knowledge of the general operational plan. Before starting your detailed examination and study/ you must take a guided orientation tour of the facility to acquaint yourself with the physical setting. Make notes on your plot plan and pad during this tour.

I. Physical Description of the Facility

• Is the facility subject to natural-disaster phenomena?
• Describe in detail the above if applicable.
• What mayor vehicular and railroad arteries serve this facility?
• How many wood-frame buildings? Describe and identify them.
• How many load-bearing brick buildings? Describe and identify them.
• How many light or heavy steel-frame buildings? Describe and identify them
• How many reinforced concrete buildings? Describe and identify them.
• Are all buildings within one perimeter? If not/ describe.

II. Perimeter Security

• Describe type of fence/ walls/ buildings/ and physical perimeter barriers.
• Is fencing of acceptable height, design, and construction?
• What is present condition of all fencing?
• Is material stored near fencing?
• Are poles or trees near fencing? If so, is height of fence increased?
• Are there any small buildings near fencing? If so, is the height of fence increased?
• Does undergrowth exist along the fencing?
• Is there an adequate clear, zone on both sides along fencing?
• Can vehicles drive up to fencing?
• Are windows of buildings on the perimeter properly secured??
• Is wire mesh on windows adequate for its purpose?
• Are there any sidewalk elevators at this facility? If so, are they properly secured when not in operation?
• How are sidewalk elevators secured during operation?

• Do storm sewers or utility tunnels breach the barrier?
• Are these sewers or tunnels adequately secured?
• Is the perimeter barrier regularly maintained and inspected?
• How many gates and doors are there on the perimeter?
• Number used by personnel (visitors, employees)?
• Number used by vehicles?
• Number used by railroad?
• How is each gate controlled?
• Are all gates adequately secured and operating properly?
• Are railroad gates supervised by the guard force during operations?
• How are the railroad gates controlled?
• Do swinging gates close without leaving a gap?
• Are gates not used. secured and sealed properly?
• What is security control of opened gates?
• Are chains and locks of adequate construction used to secure gates?
• Are any alarm devices used at the gates?
• Is CCTV used to observe gates or any part of the perimeter?
• How many doors from buildings open onto the perimeter?
• What type are they—personnel or vehicular?
• How are they secured when not in use?
• What is security control when in use?
• How many emergency doors breach the perimeter barrier?
• How are the emergency doors secured to prevent unauthorized use?
• Are there any unprotected areas on the perimeter?
• What portion of the fence does the guards observe while making rounds?

III. Building Security

A. Offices
• Where are the various administrative offices located generally?
• When are offices locked?
• Who is responsible to check security at end of day?
• How and where are company records stored?
• How are they secured?
• Are vaults equipped with temperature thermostats? (rate-of- rise/Pyro-Larm)

• Are offices equipped with sprinklers? Fire extinguishers?
• Are any central station or local alarms installed to protect safes, cabinets, etc?
• Are various file cabinets locked?
• Are individual offices locked?
• Does the company have IBM computer rooms?
• What type of fire protection are they given?

B. Plant

• When and how are exterior doors locked?
• When and how are dock doors locked?
• Are individual plant offices locked?
• Are warehouses apart from production area secured?
• Are certain critical and vulnerable areas protected by alarms? What type?
• Are locker room windows covered by screening?

C. Tool Room

• Is one or more established?
• Departmental or central tool room?
• What is the method of control and receipt?
• How is tool room secured?

D. Locker Rooms

• What is basis of issue to individual?
• What is type of locker—wall or elevated-basket type?
• How are individual lockers secured?
• Does company furnish keys/locks?
• Who or what department controls keys/locks?
• What control methods are used?
• How and when are keys and locks issued and returned?

• Are unannounced locker inspections made?
• Who conducts inspections and how often?

E. Special Areas That May Require Additional Attention (If the facility houses the following types of activities, they may require special individual inspection. Base recommendations on any or all of the applicable portions of the checklist. You will, after the initial inspection tour, design a checklist applicable to these special areas.)

• Research and development areas
• Laboratories
• Storage areas for valuable, critical, or sensitive items
• Finished product test areas
• Finished-product display areas
• Vehicle parking garages apart from the facility
• Vacant or used lofts, attics, etc.
• Mezzanines or subbasements
• Aircraft hangars, maintenance shops, and crew quarters.

IV. Security of Shipping and Receiving Areas

• How many shipping docks, vehicle and railroad?
• What are the hours of operation of docks?

• What is the method of inventory control at docks?
• What is the method of control of classified items?
• What is the security of classified or "hot" items?
• What supervision is exercised at the docks?
• Are loaded and unloaded trucks sealed?
• Who is responsible for sealing vehicles?
• What type of seals is being used?
• How are truck drivers controlled?
• Is there a designed waiting room for truck drivers?
• Is it separated from company employees?
• Are areas open to other than dock employees?
• Do guards presently supervise these areas? Is this necessary?
• What is the method of accounting for material received?
• Is shipping done by parcel post?
• What is the control at point of packaging?

• Who controls stamps or stamp machines?
• Who transports packages to post office?
• What is the method of transport to post office?
• Where is pick-up point at plant?
• What controls are exercised over the transport vehicle?
• Are inspections of operations made presently?
• Who conducts these inspections and how often?
• Does the facility have ship-loading wharves or docks?
• Are contract longshoremen used?
• How do longshoremen get to and from the docks?
• If they pass through the facility, how are they controlled?
• How are ships' company personnel controlled when given liberty?
• Are any specific routes through the facility designated for long- shoremen and ship personnel?
• If so, how is it marked and is it used?
• Are these personnel escorted?
• If they are not escorted what measures are taken to escort them?
• Is there any way in which these personnel could be kept from passing through the facility?

V. Area Security

• Can guards observe outside areas from their patrol routes?
• Do guards expose themselves to attack?
• Are patrols staggered so no pattern is established?
• What products are stored in outside areas?
• Is parking allowed inside the perimeter?
• If so, are controls established and enforced?
• Where do employees, visitors, and officials park?
• What security and control is provided?
• Are parking lots adequately secured?
• Is there a trash dump on the premises?
• How is it secured from the public?
• Is it manned by company employees?
• Is its approach directly from the manufacturing facility?
• Do roads within the perimeter present a traffic problem?
• Do rivers, canals, public thoroughfares, or railroads pass through the plant?
• Are loaded trucks left parked within the perimeter?
• If so, what protection is given them?
• Do the roads outside the facility present a traffic problem?
• What are these problems and how can they be remedied?
• Is there any recreational activity within the perimeter, such as baseball?
• Are these areas fenced off from the remainder of the property?
• Could they logically be fenced off?

VI. Protective Lighting

• Is protective lighting adequate on perimeter?
• What type of lighting is it?
• Is lighting of open areas within perimeter adequate?
• Do shadowed areas exist?
• Are outside storage areas adequately lighted?
• Are inside areas adequately lighted?
• Is the guard protected or exposed by the lighting?
• Are gates adequately lighted?
• Do lights at gate illuminate interior of vehicles?

• Are critical and vulnerable areas well illuminated?
• Is protective lighting operated manually or automatically?
• Do cones of light on perimeter overlap?
• Are perimeter lights wired in series?
• Is the lighting at shipping and receiving docks or piers adequate?
• Is lighting in the parking lots adequate?
• Is there an auxiliary power source available?
• Is the interior of buildings adequately lighted?
• Are top secret and secret activities adequately lighted?
• Are guards equipped with powerful flashlights?
• How many more and what type of lights are needed to provide adequate illumination? In what locations?
• Do security personnel report light outages?
• How soon are burned-out lights replaced?

VII. Key Control/Locking Devices, and Containers

• Is there a grandmaster, master, and submaster system? Describe it.
• Are locks used throughout the facility of the same manufacture?
• Is there a record of issuance of locks?
• Is there a record of issuance and inspection of keys?
• How many grandmaster and master keys are there in existence?
• What is the security of grandmaster and master keys?
• What is the security of the key cabinet or box?
• Who is charged with handling key control? Is the system adequate? Describe the control system.
• What is the frequency of record and key inspections?
• Are keys made at the plant?
• Do key gows have a special design?
• What is the type of lock used in facility? Are all adequate in construction?
• Would keys be difficult to duplicate?
• Are locks changed periodically at critical locations?
• Are any "sesame" padlocks used for classified material storage areas or containers?
• If a key cutting machine is used, is it properly secured?
• Are key blanks adequately secured?
• Are investigations made when master keys are lost?
• Are locks immediately replaced when keys are lost?
• Do locks have interchangeable; cores?
• Are extra cores properly safeguarded?
• Are combination locks three-position type
• Are safes located where the guard can observe them on rounds?
• How many people possess combinations to safes and containers?
• How often are combinations changed?
• What type of security containers are used for the protection of: Money? Securities? High value metals? Company proprietary material? Government classified information?
• Are lazy-man combinations used?
• Are birth dates, marriage dates, etc., used as combinations?
• Are combinations recorded anywhere in the facility where they might be accessible to an intruder?
• Are the combinations recorded and properly secured so that authorized persons can get them in emergencies?
• Is the same or greater security afforded recorded combinations as

that provided by the lock?
• Where government classified information is concerned, does each person in possession of a combination have the proper clearance and the "need to know"?
• Have all faces of the container locked with a combination lock been examined to see if combination is recorded?
• Are padlocks used on containers containing classified material chained to containers?

VIII. Control of Personnel and Vehicles

• Are passes or badges used? By whom?
• Type used? Describe in detail?
• Is colour coding used?
• Are badges uniformly worn on outer clothing?
• Are special passes issued? To whom? When?
• Who is responsible for issue and receipt of passes and badges?
• Are badges and passes in stock adequately secured?
• How are outside contractors controlled?
• How are visitors controlled?
• How are vendors controlled?
• How many employee entrances are there?
• What type of physical control is there at each entrance and exit?
• Where are the time clocks located?
• Is it possible to consolidate clock locations to one or two main clock alleys?
• Is there any control at time clock locations?
• Are there special entrances for people other than employees?
• How are the special entrances controlled?
• Are fire stairwells used for operational purposes?
• Does the facility use elevators to various floors?
• What control is exercised over their use?
• Are the elevators automatic or attended?
• Do the elevators connect operational floors and strictly office floors?
• Does this present a problem in personnel control?
• Are the elevators automatic or attended?
• If automatic, are floor directories posted in them?
• Do avenues within the buildings used for emergency egress present a problem of personnel control?
• Examine pedestrian flow from entrance, to locker room, and to work area.
• Can changes be made to shorten routes or improve control of personnel in transit?
• Are personnel using unauthorized entrances and exits?
• If government classified work is being performed, do controls in use comply with the Defense Department pamphlet for safeguarding classified information?
• Are groups authorized to visit and observe operations?
• How are these groups controlled?
• Do registers used to register visitors, vendors, etc. contain adequate information?
• Are these registers regularly inspected? By whom?
• Are employees issued uniforms?
• Are different colors used for different departments?
• What control is exercised over employees during lunch and coffee breaks?
• Do guards or watchmen ever accompany trash trucks or vending machine servicemen?
• Is parking authorized on premises within the perimeter?

• Are parking lots fenced off from the production areas?
• What method of control of personnel and vehicles is there in the parking lots?
• Is vehicle identification used?
• What type of vehicle stickers or identification is used?
• How are issue and receipt of stickers controlled?
• If executives park within the perimeter, are their autos exposed to employees?
• If nurses and doctors park within the perimeter, are their autos exposed to employees?
• Where do vendor servicemen park?
• Do vendor servicemen use plant vehicles to make the service tours? Are small vehicles available?
• How are outside-contractor vehicles controlled?
• What method is used to control shipping and receiving trucks?
• Are the parking facilities adequate at the docks?
• Does parking present a problem in vehicle or personnel control?
• What is the problem encountered?
• During what hour does switching of railroad cars occur?
• Is it possible for persons to enter the premises during switching?
• Are there adequate directional signs to direct persons to specific activities?
• Are the various buildings and activities adequately marked to preclude persons from becoming lost?
• Are safety helmets required?
• Are safety shoes required?
• Are safety glasses required?
• Are safety gloves required?
• Are safety aprons required?
• Are full-time nurses or doctors available?
• Is there a vehicle available for emergency evacuation? What type is it?

IX. Safety for Personnel

• How far away is the nearest hospital in time and distance?
• Are any company employees or guards trained in first aid?
• Is a safety director appointed?
• Is there a safety program? What does it consist of?
• How often does the safety committee meet?
• Is a first aid or medical room available?
• How are medicine cabinets secured?
• Who controls these keys?
• How is the first aid room secured?
• Are any narcotics on hand?
• If so, has narcotics security been established?
• Are the required safety equipment items worn? By visitors?
• What is the safety record of this facility?
• How does it compare with the national record?
• Are areas around machinery well policed?
• Does machinery have installed guards where needed? Are they used?
• Are mirrors used where needed to allow forklift operators to observe "blind" turns?
• Could or would mechanical devices used for forklift control improve safety?
• What type of device could be used? Pneumatic alarm system? Signal light?

X. Organization for Emergency

• Are doors adequate in number for speedy evacuation?
• Are they kept clear of obstructions and well marked?
• Are exit aisles clear of obstructions and well marked?
• Are emergency shutdown procedures developed, and is the evacuation plan in writing?
• Do employees understand the plans?
• Are emergency evacuation drills conducted?
• Do guards have specific emergency duties? Do they know these duties?
• Are local police available to assist in emergencies?
• Are any areas of the building in this facility designated as public disaster shelters?
• If so, what control is established to isolate the area from the rest of the facility?
• Do the emergency plans provide for a designated repair crew? Is the crew adequately equipped and trained?
• Are shelters available and marked for use of employees?
• If the plant is subject to natural disaster phenomena, what are they? Floods? Tornadoes?
• What emergency plans have been formulated to cope with these hazards?
• When and what was the latest incident involving a natural disaster?
• Did it result in loss of life or loss of time?
• Attach a copy of the emergency procedures.

XI. Theft Control

• Are lunchbox inspections conducted?
• Is a package-pass control system being used? Describe it.
• Is a company-employed supervisor assigned to check the package-pass system regularly?
• Is a company official occasionally present during lunchbox inspections?
• Are package passes serially numbered or otherwise containing control numbers?
• Is security of package passes in stock adequate?
• Are comparison signatures available for comparison?
• Is the list of signatures kept up to date?
• What action is taken when anyone is caught stealing?
• What controls are established on tools loaned to employees?
• What controls are established on laundry being removed?
• What is the method of removal of scrap and salvage?
• What controls are exercised over removal of useable scrap?
• Is control of this removal adequate?
• Are vending and service vehicle inspections being conducted?
• Do employees carry lunch boxes to their work areas?
• Are railroad cars inspected entering and leaving the plant?
• Are company-owned delivery or passenger vehicles authorized to park inside buildings of the plant?
• Does this parking constitute a possible theft problem?
• Do guards check outside the perimeter area for property thrown over fences?
• Do guards occasionally inspect trash pick-up? Does anyone?

XII. Security Guard Forces

• What is present guard coverage—hours per day and total hours per week?
• Describe in detail guard organization and composition.
• Number and times of shifts each twenty-four-hour period during weekdays and weekends?
• Number of stationary posts? When are they manned?
• Number of patrol routes? When and where are they, and when

are patrols made?
• Are tours supervised by ADT or DETEX stations or both?
• How many stations? Locate them on your plot plan (use different colours or shapes or symbols for different floors and routes).
• What is length of time of each patrol?
• Is there additional coverage on Saturdays, Sundays, or holidays?
• Do the patrol routes furnish adequate protection as presently established?
• Are the guards required to be deputized?
• Are armed guards required?
• How do guards communicate while on patrol?
• Are written guard instructions available? If so, secure a copy.
• If no written instructions are available, generally describe duties of each shift and post.
• What equipment does the guard force have issued? Need?
• Do they require security clearances? What degree?
• Do they require special training?
• Is there a training program in force?
• What communications are available to the guard force to call outside the facility?
• Is the number of guards, posts/ and patrol routes adequate?
• Are mechanical or electrical devices used in conjunction with the guard force?
• Do the guards know how to operate/ reset/ and monitor the devices properly?
• Do the guards know how to respond when the alarms are activated?
• Are guards included in emergency plans?
• Do guards know their duties? Emergency duties?
• Do guards make written reports of incidents?
• Are adequate records of incidents maintained?
• Are the guards familiar with the use of fire-fighting equipment?

APPENDIX E: HERSTRUKTURERING VAN NASPERS IN-HUIS SEKURITEITS DIENSTE

NASPERS

Memorandum

AAN: DIE UITVOERENDE KOMITEE
PERSONEELKOMITEE

VAN: HE1N **BRAND**

DATUM: 1 **FEBRUARIE 1999**

HERSTRUKTURERING/RASIONALISERING: SEKERHEID

Die notules van die Uitvoerende Komitee van Naspers (25 November 1998), die direksie van Nasionaie Media Beperk (1 Desember 1998) en die Personeelkomitee van Naspers Beperk (3 Desember 1998) verwys.

Aqterqrond

Beginselgoedkeuring is gegee vir die herstrukturering van sekuriteit in terme waarvan die bestaande personeel oorgedra word na 'n onafhanklike sekerheidsmaatskappy vanaf Aprii 1998.
Mnre. Brand en Barnard het opdrag ontvang om die herstrukturering te onderhandel met potensiele diensverskaffers aan die hand van bepaalde riglyne en, tesame daarmee, om 'n proses van konsultasie met die betrokke personeel te voer. Hiermee die terugvoering wat 'n aanbeveling behels van hoe die beginselbesluit implementeer kan word.

Stappe geneem

Daar is omvattend onderhande] met 'n aantal potensiele diensverskaffers en skriftelike voorstelle is ontvang en ontleed, ook wat finansiele implikasies betref.

Wat die personeel betref, is samesprekings gevoer onder toesig van Hennie du Toit van die Menslike Hulpbronne-afdeling.

Carel Barnard het ook wyd konsulteer met die besigheidseenhede in Naspers wat deur die voorgestelde rasionalisering beinvloed word.

Gevolgtrekkings

In die lig van die voorgenome rasionalisering is daar nou reeds vir 'n geruime tyd nie permanente aanstellings gemaak in die afdeling: risikobeheer nie, met die effek dat 38 van die totale personeelkompliment van 146 kontrakwerkers is.

Uit die konsultasies met personeel het dit geblyk dat daar 'n sterk voorkeur is dat die funksie eerder uitfaseer word deur gewoon nie verdere aanstellings te maak nie en daar was ook aansienlike weerstand teen die eensklapse verskuif van personeel na buite-instansies se beheer van die besigheidseenhede (kliente) se kant af.

Vanuit 'n finansiele oogpunt blyk 'n stelselmatige rasionalisering ook die beste opsie te wees.

Die aanbeveling is dus dat die rasionalisering stelselmatig infasseer word aan die hand van die volgende riglyne:

finaliseer onderhandelinge met personeel in terme waarvan die sekerheidsdienste oor 'n periode van verkieslik 3 (drie) maar nie meer as 5 (vyf)jaar uitfaseer word benewens tien persone wat vrywilllig so aangedui het, word geen ander personeel intussen uitdienstredingspakkette betaal nie. Die koste word beraam op ongeveer R120 000. Die posisie word eers heroorweeg teen die einde van die proses

alle bestaande kontrakwerkers se kontrakte wat op31 Maart verstryk, word nie hernu nie- Carel Barnard-onderhandel met 'n sekerheidsmaatskappy om daardie persone in diens te neem en te ontplooi in terme van 'n kontrak met Naspers waar personeei aftree of bedank word hul poste gevries en hulle effektief vervang deur personeel van 'n sekerheidsmaatskappy. Naspers behou die reg om inspraak te hê ten opsigte van die personeel wat sodanige sekerheidsfirma ontplooi op ons persele die enigste poste wat gevul mag word het betrekking op sekere toesighouers by die filiale. Daar word voorsien dat daar na afloop van die proses 'n klein "bevelstruktuur" in Naspers se diens sal wees om te versker dat 'n kwaliteit diens ontvang word 'n bepaling van die subkontrakteringsooreenkomste moet behels dat 'n "perseeltoelaag" of iets dergliks deur Naspers betaal word om die sekerheids-personeel direk te subsidieer. Dit word gedoen met die oog daarop om kwaliteit sekerheidspersoneel te verseker en om die personeel te onderskei van die wat diens lewer aan ander instansies.

Versoek

Dat die Uitvoerende Komitee die voorgestelde herstrukturering van sekerheidsdienste soos voorheen bespreek, bevestig. Sodanige herstrukturering vind binne 'n tydsraamwerk van 3 tot 5 jaar plaas aan die hand van kriteria soos bepaal deur die Uitvoerende Komitee soos hierbo uiteengesit.

APPENDIX F: APPROVAL LETTER FOR NASEB SECURITY PARTNERS

Nasionale Media Bpk
Naspers-Sentrum
Heerengracht 40
Kaapstad Posbus2271
Kaapstad8000 Telefoon:
(021)406-2409 Faks:
(021) 406-2457

NASPERS

National Media Ltd
Naspers Centre 40
Heerengracht Cape Town
Box 2271 Cape Town
800) Telephone (021)
406-2409 Fax**: (021)** 406-2457

11 Maart 1999

HEIL DE LESER

Hiermee bevestig ek dat ASAP A mnre G le Roux en B de Villiers se tender aanvaar word vir sekerheidsdienste vanaf 1 April 1999 vir Naspers.

C J BARNARD
GROEPBESTUURDER: EIENDOMME EN RISIKOBEHEER