TAIO
SEKE

Engineering Approach to Risk Management in Information Technology Systems

by

HARUN SEKER 920416888

Dissertation submitted in partial fulfillment of the requirements for degree

Magister Philosophiae

in the

FACULTY OF ENGINEERING and THE BUILT ENVIRONMENT

at the

UNIVERSITY OF JOHANNESBURG

SUPERVISOR: PROF. LEON PRETORIUS

February 2006

Johannesburg

ABSTRACT

The use of information systems has increased dramatically after the emergence of internet. Individuals, companies and organizations are becoming increasingly dependent on IT systems.

Before technology and computers became such an important part of society, it was difficult to manage and control large organizations. Today computers enable the effective and efficient management of large organizations, therefore allowing them to spread throughout the country and world.

Businesses are following latest advances in this era to remain competitive in the changing global market place. They use computers, automated IT systems and networks to gather, store, retrieve, process, and analyze information as well as to trade and communicate.

The rapid advances in computer technology are largely a result of the research, development and design efforts of computer engineers. There is a direct correlation between a nation's wealth and scientific and technological capacity. The most effective way of taking our country forward is to enthuse our youth for science and technology.

As the world makes rapid, sometimes breathtaking strides in the diverse fields of science and technology, South Africa more than ever needs qualified individuals who will use their skills and entrepreneurial spirit to enable our country to complete internationally with the best.

However, Information systems and networks and their worldwide increasing usage have been accompanied by new and increasing risks. Data and information stored on and transmitted over information technology systems and networks are subject to threats from various means of unauthorized access, such as misuse, misappropriation, alteration, malicious code transmissions, denial of service or destruction and require appropriate safeguards.

This research report will aim to emphasize the importance of risk management and its three activities; risk assessment, risk mitigation and evaluation and assessment. It will focus on activities that deal with the solution of problems through logical thinking, information system management

This report will also deal with a case study that gives us real life examples of risk management experiences of one local computer hardware and software supplier companies.

Information has become valuable assets that need to be protected after moving to a digital era and E-commerce. Protecting information can also be as critical as protecting other resources like money and physical assets.

ACKNOWLEDGEMENTS:

To my supervisor Prof.L.Pretorius of U.J., thank you for your interest and motivation.

To my friends, Mr.Cengiz Basar, Mr.Orhan Celik, Mr.Edip Senyurek and Mr. B. Ufuk Balci for being helpful, encouraging and supportive during preparation of this research report.

To my deputy principal Mr.Joseph Mavhunga for your time and inspiration.

To my wife for encouragement, support and understanding.

To Esquire Technologies for their permission to use their resources and my special thanks to owner of the company Mahomed Kassim.

LIST OF FIGURES

Figure 1.1 - Dollar Amount Losses by Reason
Figure 1.2 - Risk Management processes.
Figure 2.1 - SDLC phases.
Figure 3.1 - Risk Assessment Methodology Flowchart
Figure 4.1 - Risk Mitigation Action Points.[adapted from
Figure 4.2 - Risk Mitigation Methodology Flowchart
Figure 4.3 – Technical Security Controls
Figure 4.4 - Implemented Controls and Residual Risk
Figure 6.1 - A view of Fincon Accounting Software
Figure 6.2 - Esquire Network
Figure 6.3 - New Esquire Network

LIST OF TABLES

Table 1.1 - World Internet Usage and Population Statistics
Table 1.2 - Dollar Amount Losses by Reason
Table 2.1 - Integration of Risk Management into the SDLC
Table 3.1 - Human Threats: Threat-Source, Reasons, and Threat Actions
Table 3.2 - Vulnerability / Threat Pairs
Table 3.3 - Security Criteria
Table 3.4 - Likelihood Definitions
Table 3.5 - Magnitude of Impact Definitions
Table 3.6 - Risk-Level Matrix
Table 3.7 - Risk Level and Necessary Actions

LIST OF ACRONYMS

DAA	Designated Approving Authority
DAC	Discretionary Access Control
E-commerce	Electronic Commerce
Fed CIRC	Federal Computer Incident Response Center
FTP	File Transfer Protocol
IT	Information Technology
ICT	Information and Communication Technology
ISSO	Information Security Officer
MAC	Mandatory Access Control
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PC	Personal Computer
SDLC	System Development Life Cycle

TABLE OF CONTENTS

Abstract..... I

Acknowledgements..... III

List of Tables..... IV

List of Figures..... V

List of Acronyms..... VI

Table of Contents VII

CHAPTER 1 1

INTRODUCTION AND RESEARCH PROPOSAL 1

1.1. Introduction 1

1.2. Problem Statement 5

1.3. Research Objectives 5

1.4. Research Approach and Presentation Structure..... 5

1.5. Conclusion 6

CHAPTER 2..... 7

RISK MANAGEMENT OVERVIEW..... 7

2.1. Importance of Risk management 7

2.2. Integration of Risk management into SDLC 9

2.3. Key Roles of the Personnel 11

2.4. Conclusion 12

CHAPTER 3..... 13

RISK ASSESSMENT 13

3.1. Introduction..... 13

3.1.1. Step 1 – System characterization 15

3.1.2. Step 2 – Threat Identification 16

3.1.3. Step 3 – Vulnerability Identification 18

3.1.3.1 – Finding Vulnerability Sources 19

3.1.3.2 – System Security Testing 19

3.1.3.3 – Development of Security Requirements Checklist..... 20

3.1.4. Step 4 – Control Analysis 21

3.1.4.1 – Control Methods 21

3.1.4.2 – Control Categories 21

3.1.4.3 – Control Analysis Technique 21

3.1.5. Step 5 – Likelihood Determination 22
3.1.6. Step 6 – Impact Analysis 22
3.1.7. Step 7 – Risk Determination 23
3.1.8 Step 8 – Control Recommendation 24
3.1.9. Step 9 – Result Documentation 24
3.2. Conclusion 25
CHAPTER 4 26
RISK MITIGATION 26
4.1. Introduction 26
4.2. Risk Mitigation Options 27
4.3. The Risk Mitigation Strategy 27
4.4. An Approach for Control Implementation 29
4.5. Control Categories 30
4.5.1. Technical Security Controls 31
4.5.1.1. Supporting Technical Controls 32
4.5.1.2. Preventive Technical Controls 32
4.5.1.3. Detection and Recovery Technical Controls 33
4.5.2. Management Security Controls 34
4.5.2.1. Preventive Management Security Controls 34
4.5.2.2. Detection Management Security Controls 34
4.5.2.3. Recovery Management Security Controls 35
4.5.3. Operational security Controls 35
4.5.3.1. Preventive Operational Controls 35
4.5.3.2. Detection Operational Controls 36
4.6. The Cost Benefit Analysis 36
4.7. Residual Risk 37
4.8. Conclusion 37
CHAPTER 5 38
RISK EVALUATION AND ASSESSMENT 38
5.1. Introduction 38
5.2. Conclusion 41
CHAPTER 6 42
CASE STUDY 42
6.1. Company Overview and Introduction 42

6.2. Risk Management of Esquire technologies..... 46
6.3. Conclusion..... 50
CHAPTER 7..... 51
CONCLUSION AND RECOMMENDATION..... 51
6.1. Conclusion..... 51
6.2. Recommendation 53
REFERENCES..... 54

CHAPTER 1

INTRODUCTION AND RESEARCH PROPOSAL

"Do not leave everything to the police. Make sure you pay enough attention to your company's IT security." ***Professor Les Labuschagne*** *(Deputy Chairperson of the department of information technology (IT) management of the University of Johannesburg Academy for IT) [16]*

1.1. INTRODUCTION

In this century of information, individuals, companies and organizations are becoming increasingly dependent on computers and automated IT systems to fulfill many basic functions. [5] Businesses are using and also following latest advances in this era to remain competitive in the changing global market place. They use computers and automated IT systems to gather, store, retrieve, process, and analyze information as well as to trade and communicate. [2]

The latest advances in IT systems have reduced the costs of managing information, individuals and organizations have undertaken information-related tasks more efficiently, and innovations in products and processes have been introduced. [26]

The usage of the internet has increased significantly as shown in the table 1.1. since the mid-1990's. Because of this, the internet has solidified the central role of computers in the functioning of modern organizations. IT security has also moved to centre stage after the emergence of internet. [12]

WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	**Population (2006 Est.)**	**Population % of World**	**Internet Usage, Latest Data**	**% Population (Penetration)**	**Usage % of World**	**Usage Growth 2000-2005**
Africa	915,210,928	14.1 %	22,737,500	2.5 %	2.2 %	403.7 %
Asia	3,667,774,066	56.4 %	364,270,713	9.9 %	35.7 %	218.7 %
Europe	807,289,020	12.4 %	290,121,957	35.9 %	28.5 %	176.1 %
Middle East	190,084,161	2.9 %	18,203,500	9.6 %	1.8 %	454.2 %
North America	331,473,276	5.1 %	225,801,428	68.1 %	22.2 %	108.9 %
Latin America/Caribbean	553,908,632	8.5 %	79,033,597	14.3 %	7.8 %	337.4 %
Oceania / Australia	33,956,977	0.5 %	17,690,762	52.9 %	1.8 %	132.2 %
WORLD TOTAL	6,499,697,060	100.0 %	**1,018,057,389**	15.7 %	100.0 %	182.0 %

Internet Usage and World Population Statistics were updated on December 31, 2005.

Table 1.1 - World Internet Usage and Population Statistics [adapted from 15]

Information has become a valuable asset that needs to be protected after moving to a digital era and E-commerce. Protecting information can be as critical as protecting other resources like money and physical assets. [4]

Since the information is as valuable as money, it has created a new area for crime .This type of crime which uses a computer to steal, embezzle, or defraud is called computer crime or cyber crime. [19] This is the name given to any type of electronic fraud. It covers credit and debit cards, electronic funds transfers, software piracy and any other general misuse of a computer system. [20] Computer Crime, E-Crime, Hi-Tech Crime or Electronic Crime is a crime in which computers play an essential part. [21]

The Computer Security Institute, in conjunction with the FBI conducted a Crime and Security survey in the USA in 2005. The finding was that losses caused by computer security incidents amounted to $130,104,542 compared to $141, 49-million in 2004 and $201, 79-million in 2003. [12]

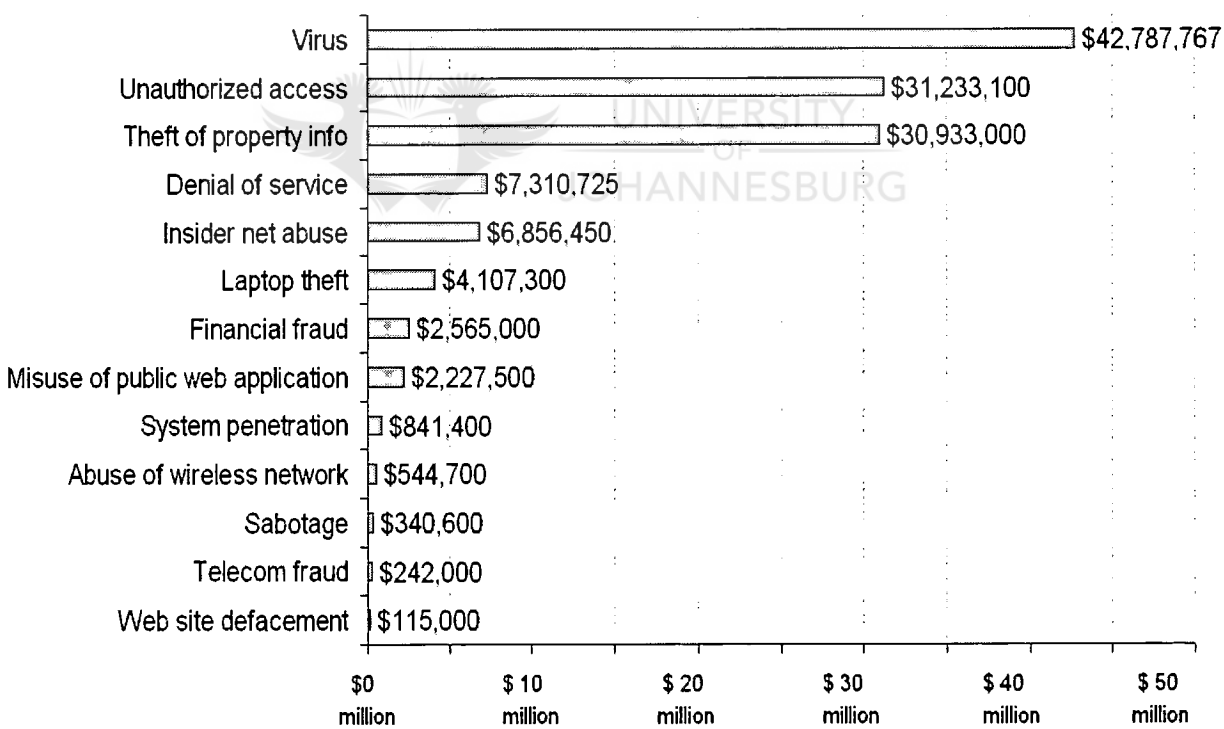

Figure 1.1 - Dollar Amount Losses by Reason [adapted from 12]

Reason of Losses	Amount
Virus	$42,787,767
Unauthorized access	$31,233,100
Theft of property info	$30,933,000
Denial of service	$7,310,725
Insider net abuse	$6,856,450
Laptop theft	$4,107,300
Financial fraud	$2,565,000
Misuse of public web application	$2,227,500
System penetration	$841,400
Abuse of wireless network	$544,700
Sabotage	$340,600
Telecom fraud	$242,000
Web site defacement	$115,000
Total	**$130,104,542**

Table 1.2 - Dollar Amount Losses by Reason [adapted from 12]

Around 639 companies took part in the survey, with only more than half providing dollar-loss estimates. Compared to 2004 and 2003, Trends of losses are down, but on the other hand there are two areas of increase. These are unauthorized access to information and theft of information.[12]

These findings clearly show that economic, financial and risk management aspects of information technology security have become important concerns to organizations. Risk management has therefore started to play a critical role in protecting companies' information assets. [12], [17]

An effective risk management process is an important component of a successful IT security program. To manage IT related risks effectively, the organizations have to identify possible risks, assess these risks and reduce them to an acceptable level. [1], [2]

1.2. PROBLEM STATEMENT

The use of information technology (IT) by organizations has potential risks. In this research, it is attempted to identify these risks and the way they can be reduced to acceptable levels.

1.3. RESEARCH OBJECTIVES

This report will first of all explain the importance of risk management and then the possible risks during the System Development Life Cycle (SDLC).

The next stage will discuss these risks in some detail and then come up with the methods to mitigate them. The following part will focus on the need for ongoing evaluation and assessment and the factors which lead to a successful risk management program.

It will be followed by a case study of risk management by Esquire Technologies, one of the largest local computer hardware and software supplier company.

1.4. RESEARCH APPROACH AND PRESENTATION STRUCTURE

The research results will be presented in 6 chapters as follows:

Chapter 1: Introduction and Research Proposal
Chapter 1 will explain the research topic and highlight the aims and objectives of the research.

Chapter 2: Risk Management Overview
It will provide an overview of risk management, how it is integrated into SDLC (System Development Life Cycle) and the role of individuals who support and use this process.

Chapter 3: Risk Assessment
This chapter assesses the risks in order to determine the extent of the threat and the risk associated with an IT system throughout its SDLC (System Development Life Cycle) and the nine steps of risk assessment methodology.

Chapter 4: Risk Mitigation

This chapter will address the options and strategies that can be employed to reduce potential risks to acceptable level.

Chapter 5: Evaluation and Assessment

This chapter focuses on the need for ongoing evaluation and assessment of the risks and possible intervention strategies which will lead to a successful management program..

Chapter 6: Case Study

This case chapter deals with a case study which will provide real life examples of risk management experiences of one local computer hardware and software supplier company.

Chapter 7: Conclusion

This chapter will be a rounding up of the arguments presented in the previous chapter.

1.5. CONCLUSION

The aim of IT risk management is to make sure well-informed risk management decisions are made by management to accomplish organization's mission and to run smoothly by securing IT systems. Risk management has three processes. These are identifying risk, assessing risk and reducing it to an acceptable level. The risk management process has three major components, also illustrated in Figure 1.2.

1. risk assessment
2. risk mitigation
3. Evaluation and assessment.

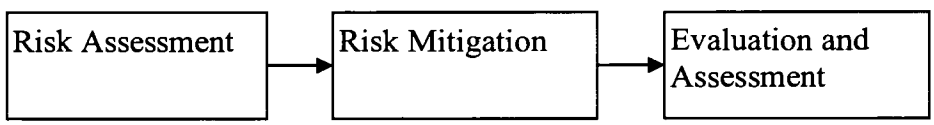

Figure 1.2 – Risk Management processes.

Risk is an inevitable part of all businesses. Risk can't be eliminated completely but can be reduced to an acceptable level. This is where risk management plays an important role. [2], [6]

CHAPTER 2

RISK MANAGEMENT OVERVIEW

"Thus far, the majority of South African companies have only done enough to cover themselves. However, what if something happens, such as a virus, or e-fraud, and there exists evidence that this was due to directors' negligence in putting in place IT security best practice? Most companies outsource their IT functions. However, when it comes to IT security, it is advisable that this must not be outsourced. You can outsource technical functions, but you cannot outsource managing your IT risk." ***Labuschagne.*** *[16]*

2.1. IMPORTANCE OF RISK MANAGEMENT

Information technology systems and networks are becoming increasingly useful and valuable to governments, businesses, other organizations and individual users. This growing dependence on IT calls for special efforts to protect and foster confidence in them in order to ensure stable and efficient national economies, and international trade and in social, cultural and political life call. [5]

The easy access to information systems and networks and their worldwide increase have been accompanied by new and increasing risks. Data and information stored on and transmitted over information technology systems and networks are subject to threats from various means of unauthorized access, such as misuse, misappropriation, alteration, malicious code transmissions and denial of service or destruction and therefore require appropriate safeguards. [5]

There is also a need to raise awareness of these risks to information systems and networks, as well as corresponding the policies, practices, measures and procedures available to respond to these risks, and to encourage appropriate safeguards. [5]

Many small and medium-sized business owners think that larger corporations are more vulnerable to internet security threats. The following example will show that it is often the

other way around. According to the Internet Security Alliance, a non-profit organization that provides a forum for information security issues, the destructive Mydoom worm affected one out of three small and medium-sized businesses, and only one out of six large enterprises,. [10]

Many small business owners don't adequately protect their computers and networks from spyware, viruses, worms, hacker attacks, customer data theft and other security threats. They do not even make the issue a priority and the result is that nearly half of all small and medium-sized businesses have not even taken the most basic security precautions, such as installing antivirus and anti-spyware programs. [10]

Why Small and Medium-sized Businesses are at Risk

There are several reasons why computers, network and the data that resides on them are at greater risk now than ever before.

- **Large networks are harder to breach.** Criminals are increasingly turning their attentions toward easier hacker targets like small and medium-sized businesses because they are easier to breach.
- **Hackers want soft targets.** Many hackers now have software tools that constantly search the internet for unprotected networks and computers. If they succeed , they can access and control these unprotected computers to launch attack on the other computers or networks.
- **Threats are becoming increasingly dangerous.** Spyware authors are busy creating very harmful programs that resist removal, perpetually mutate, and spread across the internet in minutes. Meanwhile, blended threats, which assume multiple forms and can attack systems in many different ways, are on the rise. Small businesses without adequate, updated security solutions can easily be victimized by these and other threats.
- **Insider threats.** Surveys have shown that most damage is done by insiders, people who have authorized access to a computer network. They may do this either intentionally or unintentionally. For example, an employee may unknowingly download spyware while surfing net, playing an online game or downloading unknown software.

- **Small companies are in danger.** Small businesses often lack the financial resources that large companies have to deal with security attacks. Suppose one is an online retailer and a hacker launches a denial-of-service attack against one's website. One will not have the necessary insurance or funds to recover from the subsequent loss of revenue--not to mention the damage to one's business's reputation? [10]

South Africans have stopped trading with Kenyans through the internet due to a rise in cyber crime. They have also shunned Nigeria and Indonesia for similar reasons. Mr. Matthew White, the chief Executive Officer of Iowa Press Services, said "You can send products to Nigeria, Kenya or Indonesia for an order made through internet and never get paid for it." at Annual African Computing And Telecommunication Summit 2005 in Johannesburg.[9]

He warned businesses and banks to watch out for cyber crime to avoid losses to fraudsters. He said many banks had lost millions of dollars through fraud and interception of transactions on the internet. [9]

White said that technology market research group Gartner had predicted that 60 % of security breach costs incurred by businesses are perpetrated by company insiders who are working alone or in conspiracy with outsiders. [9]

2.2 INTEGRATION OF RISK MANAGEMENT INTO SDLC

Effective risk management should be integrated into SDLC phases. Table 2.1 describes the characteristics of each phase and risk management activities that can be done during these phases. An IT system's SDLC has typically 5 phases as shown in the figure 2.1

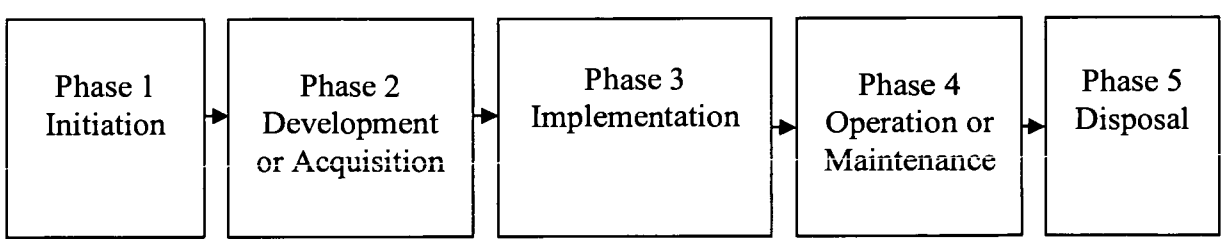

Figure 2.1 – SDLC phases. [adapted from 1]

Phases	Phase Characteristics	Risk management Activities
Phase 1: Initiation	In this phase the need for IT system is explained and also aims and scope of IT system is documented.	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2 : Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise Constructed.	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development.
Phase 3 : Implementation	The system security features should be configured, enabled, tested, and verified.	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational Environment. Decisions regarding risks identified must be made prior to system operation.
Phase 4 : Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures.	Risk management activities are performed for periodic system reauthorization (or reaccredidation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5 : Disposal	This phase may involve the disposition of information, Hardware and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software.	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner.

Table 2.1 - Integration of Risk Management into the SDLC [adapted from 1]

2.3. KEY ROLES OF THE PERSONNEL

Risk management is a fundamental management responsibility. In this section, the key roles of the personnel who should support and be involved in the risk management process are described.

- **Senior Management:** they are ultimately responsible for mission accomplishment, so that they must ensure necessary sources applied to accomplish the mission.

- **Chief Information Officers:** they are responsible for planning, budgeting and performance of IT, as well as IT security components, so that decisions made here could be based on effective risk management program.

- **System and Information Owners:** they are responsible for ensuring that proper controls are in place for the integrity and confidentiality of the IT systems and data. They have a authority to approve and sign off any hardware and software changes to their IT systems. Therefore he or she must fully support risk management programs.

- **Business and Functional Managers:** they are responsible for business operations and IT procurement process. These managers have authority and responsibility to make trade-off decisions essential to mission accomplishment. These decisions may provide effective solutions with a minimal cost.

- **ISSO (IT Security Program Manager and Computer Security Officers):** they are responsible for security programs and the risk management process. Therefore, they play a leading role in all risk management processes. They are also a major ally in support of senior management.
- **It Security Practitioners:** they are in charge of proper implementation of security requirements in their IT systems (e.g., network, system and database administrator; computer specialists; security analysts and consultants), whenever the changes occur in the system, they must support or use risk management processes to identify and assess new potential risks and implement new security controls to safeguard their IT systems.

- **Security Awareness Trainers:** they are in charge of training the organization's personnel to use the IT system and data according to policies, guidelines and the rules of behavior which is critical to mitigate risk and protect the organization's IT resources. To minimize the risks, it is essential that system and application users should be provided with security awareness programs.[1]

2.4. CONCLUSION

Risk is an inevitable part of today's businesses; absolute security is an unrealistic goal. A natural disaster or an adversary with sufficient resources and ingenuity is enough to compromise the most secure systems. [2]

IT Risk management is best managed if planned for throughout the system development life cycle.

Since zero risk is impractical or close to impossible, the objectives of IT risk management can be defined as follows:

- To make sure that the organization can accomplish its mission by securing IT systems.
- To inform management to make necessary risk management decision on a realistic IT budget.
- To inform management on the performance and effectiveness of risk management.

IT Risk management is a fundamental management responsibility. It requires the support and involvement of senior management. IT Risk management allows IT managers to balance the operational and economic costs of protective measures by selecting cost-effective security controls. [1]

These controls can be used to mitigate for the better protection of mission-critical information and the IT systems that process, store and carry information. [2]

The next chapter will describe the extent of the potential threat, the risk associated with an IT system throughout its SDLC and the nine steps of risk assessment methodology.

CHAPTER 3

RISK ASSESSMENT

> *"There can be no vulnerability without risk; there can be no community without vulnerability; there can be no peace, and ultimately no life, without community."*
> ***M. Scott peck** [22]*

3.1. INTRODUCTION

Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization. [1]

Risk assessment is the first step in IT risk management methodology. It is used to determine the extent of the potential threat and risk associated with an IT system throughout its SDLC. [1], [4]

The IT Risk Assessment methodology generally encompasses nine steps which are going to be addressed in this chapter. These steps are also expanded in figure 3.1.

- Step 1- System Characterization
- Step 2 - Threat Identification
- Step 3 - Vulnerability Identification
- Step 4 - Control Analysis
- Step 5 - Likelihood Determination
- Step 6 - Impact Analysis
- Step 7 - Risk Determination
- Step 8 - Control Recommendations
- Step 9 - Results Documentation

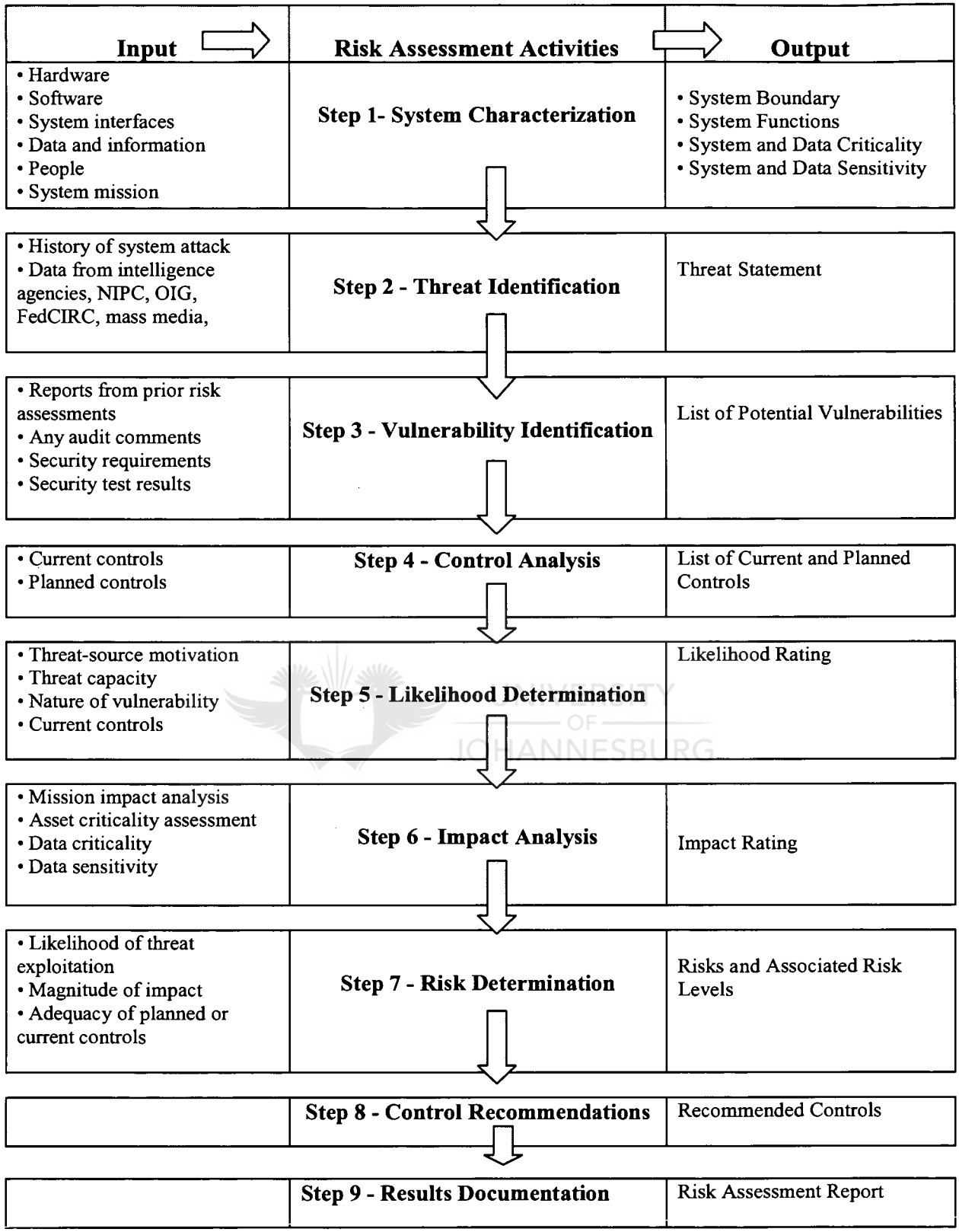

Figure 3.1 - Risk Assessment Methodology Flowchart [adapted from 1]

3.1.1. Step 1 - System Characterization

The aim of this step is to characterize the IT system and get enough information on IT system environment and delineation of system boundary. To do this, there is a need to collect the system related information which is usually classified as follows:

- System mission (the processes performed by the IT system)
- System and data criticality (the system's value or importance to an organization)
- System and data sensitivity.
- The functional requirements of the IT system
- Hardware and Software
- System interfaces.
- Data and information.
- System users who provide technical support to the IT system and application users who use the IT system to perform business functions)
- System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
- System security architecture.
- Current network topology (e.g., network diagram)
- Information storage protection that safeguards system and data availability, integrity, and confidentiality.
- Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)
- Technical controls used for the IT system
- Management controls used for the IT system
- Operational controls used for the IT system
- Physical security environment of the IT system
- Environmental security implemented for the IT system processing environment.[1], [2], [3], [4]

The following techniques can be used to gather information related to the IT system within operational boundary.

- Questionnaire.
- On-site interview.
- Document review.
- Use of automated scanning tool. [1]

3.1.2. Step 2 - Threat Identification

A threat can be simply defined as the potential for a particular threat-source to successfully exercise a particular vulnerability. [1], [4]

Vulnerability can be defined as a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. [1], [4]

The aim of this step is to list threat sources that could exploit systems' vulnerability. The common threat sources are natural, human and environmental. These threats can be explained as follows:

- **Natural Threats:** Earthquakes, Floods, tornadoes, landslides, avalanches, electrical storms, and other such events.
- **Human Threats:** These are the events caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
- **Environmental Threats:** There can also be threats posed by the unpredictable environment we live in such as long-term power failure, pollution, chemicals, and liquid leakage. [1], [4]

Information on known natural and environmental threats is readily available, whereas information on human threats should be updated on a regular basis because of the emergence of new types of human threats.

Table 3.1 presents an overview of many of today's common human threats, their possible reasons and the methods or threat action by which they might carry out an attack on IT system.

Threat-Source	Reasons	Threat Actions
Hacker, cracker	• Challenge • Ego • Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	• Destruction of information • Illegal information disclosure • Monetary gain • Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	• Blackmail • Destruction • Exploitation • Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage • Companies • Foreign governments • Other government interests	• Competitive advantage • Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access
Insiders • Poorly trained • Disgruntled • Malicious • Negligent • Dishonest • Terminated employees.	• Curiosity • Ego • Intelligence • Monetary gain • Revenge • Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Table 3.1 - Human Threats: Threat-Source, Reasons, and Threat Actions [adapted from 1]

The threat statement or list of potential threat sources should be tailored to the individual organization's needs and its processing environment.

Sources of information on threats include, but are not limited to the following:

- Intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Center)
- Federal Computer Incident Response Center (FedCIRC)
- Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.

3.1.3. Step 3 - Vulnerability Identification

Vulnerability can be described as a flaw or weakness in system security procedures, design, implementation, or internal controls, that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. [1]

The aim of this step is to develop a list of system vulnerabilities that could be exploited by the potential threat-sources.

Vulnerability	Threat Source	Threat Action
Terminated employees' system identifiers (ID) are not removed From the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on ABC server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to ABC server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system.	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities.
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

Table 3.2. - Vulnerability / Threat Pairs [adapted from 1]

Recommended methods for identification of system vulnerability are:

- Finding Vulnerability Sources
- System Security Testing
- Development of Security Requirements Checklist

3.1.3.1. Finding Vulnerability Sources

Vulnerability sources can be identified via information gathering technique as discussed in the system characterization step. Other ways of finding vulnerability sources can be as follows:

- The internet on known systems vulnerabilities posted by vendors and also hot fixes, service packs, patches and other remedial measures can be found.
- Vendor web pages that identify system bugs and flaws.
- Previous risk assessment document.
- The IT system's audit report.
- Vulnerability lists, such as the NIST I-CAT database available on http://icat.nist.gov
- System software security analyses. [1], [4]

3.1.3.2. System Security Testing

System testing can be used to identify system vulnerabilities efficiently. These test methods are as follows:

- **Vulnerability scanning tool:** it is used to scan the system for known vulnerable services like anonymous File Transfer Protocol (FTP) and send mail relaying. However this testing method is not an efficient way to find serious vulnerabilities.
- **Security test and evaluation:** it is used to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standard.
- **Penetration testing:** it is used to test the system from the view point of a threat source and also identifies potential failures in the system, so that it ensures that different facets of the IT are secured.[1], [4]

3.1.3.3. Development of Security Requirements Checklist

This is the stage in which risk assessment personnel prepare security requirement checklist in table form to determine whether the security requirements predetermined for IT system and collected during system characterization are in line with existing and planned security controls.

A security requirements checklist contains the basic security standards that can be used to evaluate and identify the vulnerabilities of the whole system in the following security areas:

- Management
- Operational
- Technical.

Security criteria suggested to identify IT system's vulnerabilities in each security area are shown in table 3.3.

Security Area	Security Criteria
Management Security	• Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • Personnel clearance and background investigations • Risk assessment • Security and technical training • Separation of duties • System authorization and reauthorization • System or application security plan
Operational Security	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (e.g., computer room, data center, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers
Technical Security	• Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

Table 3.3 - Security Criteria [adapted from 1]

3.1.4. Step 4 - Control Analysis

The aim of this step is to analyze the current controls and those planned for implementation to minimize or eliminate the likelihood of a threat that may cause vulnerability.

To obtain an overall likelihood rating, the implementation of current or planned controls must be considered. In the following sections, control methods, control categories and control analysis techniques are discussed respectively. [1], [4]

3.1.4.1. Control methods

Security controls encompass the use of technical and nontechnical methods.

Technical controls are safeguards that are built into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods and intrusion detection software).

Non-technical controls are management and operational controls, such as security policies, operational procedures, personnel and physical and environmental security. [1], [4]

3.1.4.2. Control Categories

Control categories can be classified as preventive and detective.

- **Preventative controls** prevent attempt to attack or harm security policy and include such measures as access control enforcement, encryption, and authentication.
- **Detective controls** warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums. [1], [4]

3.1.4.3. Control Analysis Technique

As was discussed in section 3.3.3 security requirement checklist will be helpful in analyzing controls in an efficient and systematic manner. This checklist can be used to validate security noncompliance as well as compliance. Therefore, it is necessary to update such checklist to reflect in security policies, methods and requirements to make sure of the checklist's validity. [1], [4]

3.1.5. Step 5 - Likelihood Determination

The aim of this step is to derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the associated threat environment. To do this the following factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

Likelihood levels as shown in the table–3.4 below can be described as high, medium, or low.

Likelihood Level	Likelihood Definition
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

Table 3.4 - Likelihood Definitions [adapted from1]

3.1.6. Step 6 - Impact Analysis

The aim of this step is to decide on magnitude of impact. Before doing this one need the following information:

- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity.[1], [4]

Magnitude of Impact	Impact Definition (Exercise of Vulnerability)
Low	(1) Results may be loss of some assets or resources or (2) May noticeably affect an organization's mission, reputation, or interest.
Medium	1) Results may be high cost losses of assets or resources; 2) May violate, harm, or impede an organization's mission, reputation, or interest; or 3) May result in human injury.
High	1) Results may be high cost losses of major assets or resources; 2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or 3) May result in human death or serious injury.

Table 3.5 - Magnitude of Impact Definitions [adapted from 1]

3.1.7. Step 7 - Risk Determination

The aim of this step is to assess the level of risk to an IT system and to develop risk scale and a risk-level matrix measure risks.

Threat Likelihood	Impact		
	Low (10)	**Medium (50)**	**High (100)**
High (1.0)	**Low** 10 x 1.0 = 10	**Medium** 50 x 1.0 = 50	**High** 100 x 1.0 = 100
Medium (0.5)	**Low** 10 x 0.5 = 5	**Medium** 50 x 0.5 = 25	**High** 100 x 0.5 = 50
Low (0.1)	**Low** 10 x 0.1 = 1	**Medium** 50 x 0.1 = 5	**High** 100 x 0.1 = 10

Table 3.6 - Risk-Level Matrix

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Risk Level	Necessary Actions
Low	The system's DAA must determine whether corrective actions are still required or decide to accept the risk.
Medium	Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
High	There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.

Table 3.7 - Risk Level and Necessary Actions [adapted from 1]

Risk level and necessary actions table presents actions that management must take.

3.1.8. Step 8 - Control Recommendations

The objective here is to provide control recommendations or alternative solutions to mitigate risks to an acceptable level. To do this the following factors should be considered:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

The goal of this step is to reduce risks to an acceptable level. To achieve this, all recommended control measures should be implemented. But, to determine the appropriate one required for a specific organization, a cost-benefit analysis should be conducted. Moreover, the operational impact and feasibility of the option should be evaluated carefully at this step. [1], [4]

3.1.9. Step 9 - Results Documentation

After covering the steps in risk management the result should be documented in a report. A risk assessment report is essential to senior management to make informed decisions on policy, procedural, budget and system operational and management changes. This report describes threats and vulnerabilities, measures the risks and provides recommendations for control implementation. [1], [4]

3.2. CONCLUSION

This chapter has highlighted some aspects which users of systems and networks need to seriously consider in assessing the risks to IT systems. It is clear that every user can be vulnerable to both natural and human threats to IT. This therefore requires management to consciously adopt a risk management methodology and then come up with control measures that will minimize risks.

The next chapter will outline the appropriate risk reducing control methods which are recommended for implementation by organizations that rely on IT systems.

CHAPTER 4

RISK MITIGATION

"If we don't act now to safeguard our privacy, we could all become victims of identity theft." ***Bill Nelson.*** *[23]*

4.1. INTRODUCTION

Risk mitigation is the second process of risk management. In this process, the appropriate risk-reducing controls which are recommended from the risk assessment process will be prioritized, evaluated and implemented. [1], [4]

Since the elimination of all risks is impractical or close to impossible, it is the responsibility of management to make decision on the least-cost approach and implement the most appropriate controls to decrease risks to an acceptable level, with minimum adverse impact on the organization's resources and mission. [1], [2], [3], [4]

In this chapter, the following will be described:

- Risk mitigation options.
- The risk mitigation strategy
- An approach for control implementation.
- Control categories.
- The cost-benefit analysis.
- Residual risk.

4.2. RISK MITIGATION OPTIONS

Risk mitigation can be achieved by implementing some of the following risk options:

• **Risk Assumption.** The potential risks will be accepted and operating the IT system will continue or controls will be implemented to reduce the risk to an acceptable level.

• **Risk Avoidance.** Causes and consequences of risk will be eliminated.

• **Risk Limitation.** Controls that minimize the adverse impact of a threat's exercising vulnerability will be implemented (e.g., use of supporting, preventative, detective controls).

• **Risk Planning.** A risk mitigation plan that prioritizes, implements, and maintains controls will be developed.

• **Research and Acknowledgment.** The risk of loss will be reduced by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.

• **Risk Transference.** Other options to compensate for the loss, such as purchasing insurance will be used. [1], [4]

4.3. THE RISK MITIGATION STRATEGY

This section addresses following questions

- When shall we take action?
- When shall we implement these controls to mitigate the risk?

Figure 4.1 addresses some of these questions

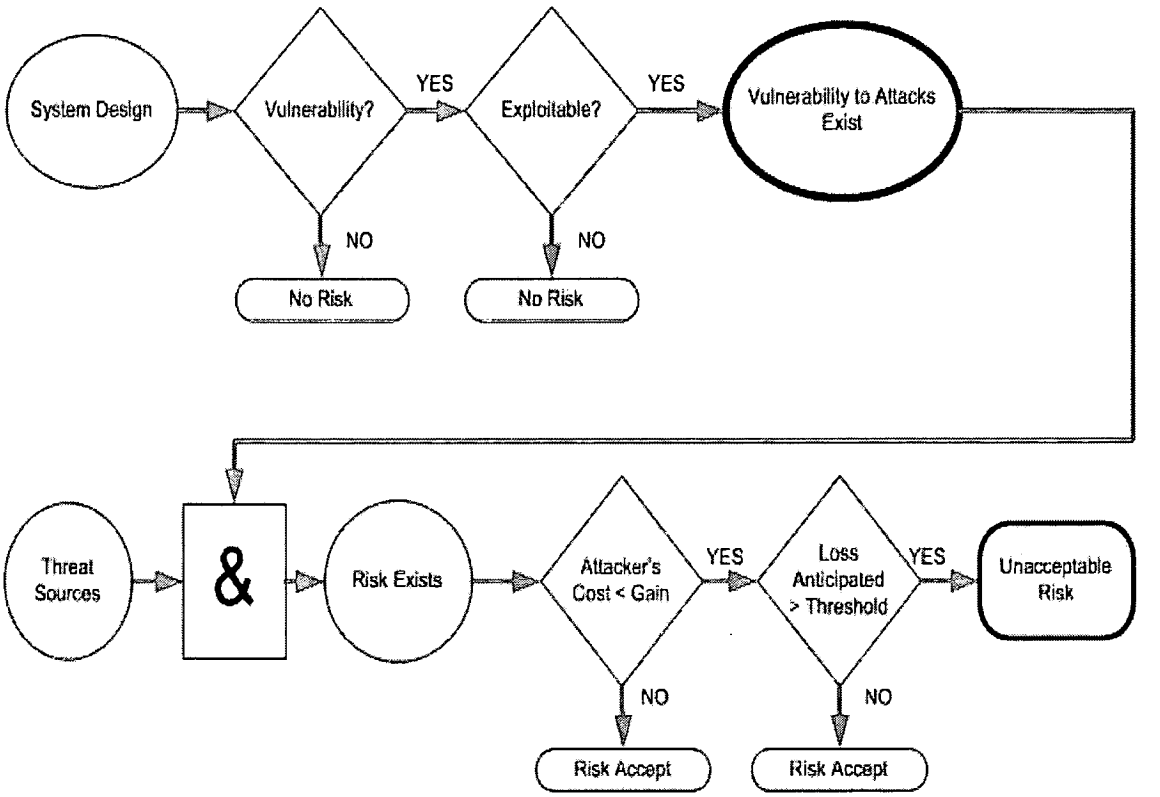

Figure 4.1 - Risk Mitigation Action Points.[adapted from 1]

• **If vulnerability exists** □ Assurance techniques will be implemented to reduce the likelihood of vulnerability's being exercised.

• **If vulnerability can be exercised** □ Layered protections, architectural designs, and administrative controls will be applied to minimize the risk of or prevent this occurrence.

• **if the attacker's cost is less than the potential gain** □ Necessary protective measures will be applied to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).

• **If loss is too great** □ Design principles, architectural designs, and technical and non-technical protections will be applied to limit the extent of the attack, so that it will reduce the potential for loss. [1]

4.4. AN APPROACH FOR CONTROL IMPLEMENTATION

Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities. [1]

The following are steps that can be followed to minimize the risks.

Step 1 - Prioritize Actions: According to the risk assessment report, implementation actions are prioritized from high to low. Top priority is given to high risks.

Step 2 - Evaluate Recommended Control Options: Recommended control options from risk assessment process are analyzed according to the feasibility and effectiveness to select the most appropriate one. List of feasible controls will be created.

Step 3 - Conduct Cost-Benefit Analysis: A cost benefit analysis is conducted to find out cost-effective controls which will assist management in decision making.

Step 4 - Select Control: Management determines the most cost effective controls based on the cost benefit analysis.

Step 5 - Assign Responsibility: Appropriate persons are identified and assigned to implement selected controls.

Step 6 - Develop a Safeguard Implementation Plan:

Safeguard implementation plan is developed based on the following in formations:

- Lists of responsible teams and staff.
- Risks and associated risk levels.
- Recommended controls, selected planned controls and prioritized actions.
- Required resources for implementing the selected planned controls.
- Start date and target completion date for implementation.
- Maintenance requirements.

Step 7 - Implement Selected Control(s)

Implementing controls may reduce the risk but can not eliminate it totally. Residual risks will be addressed in section 4.6 [1], [4]

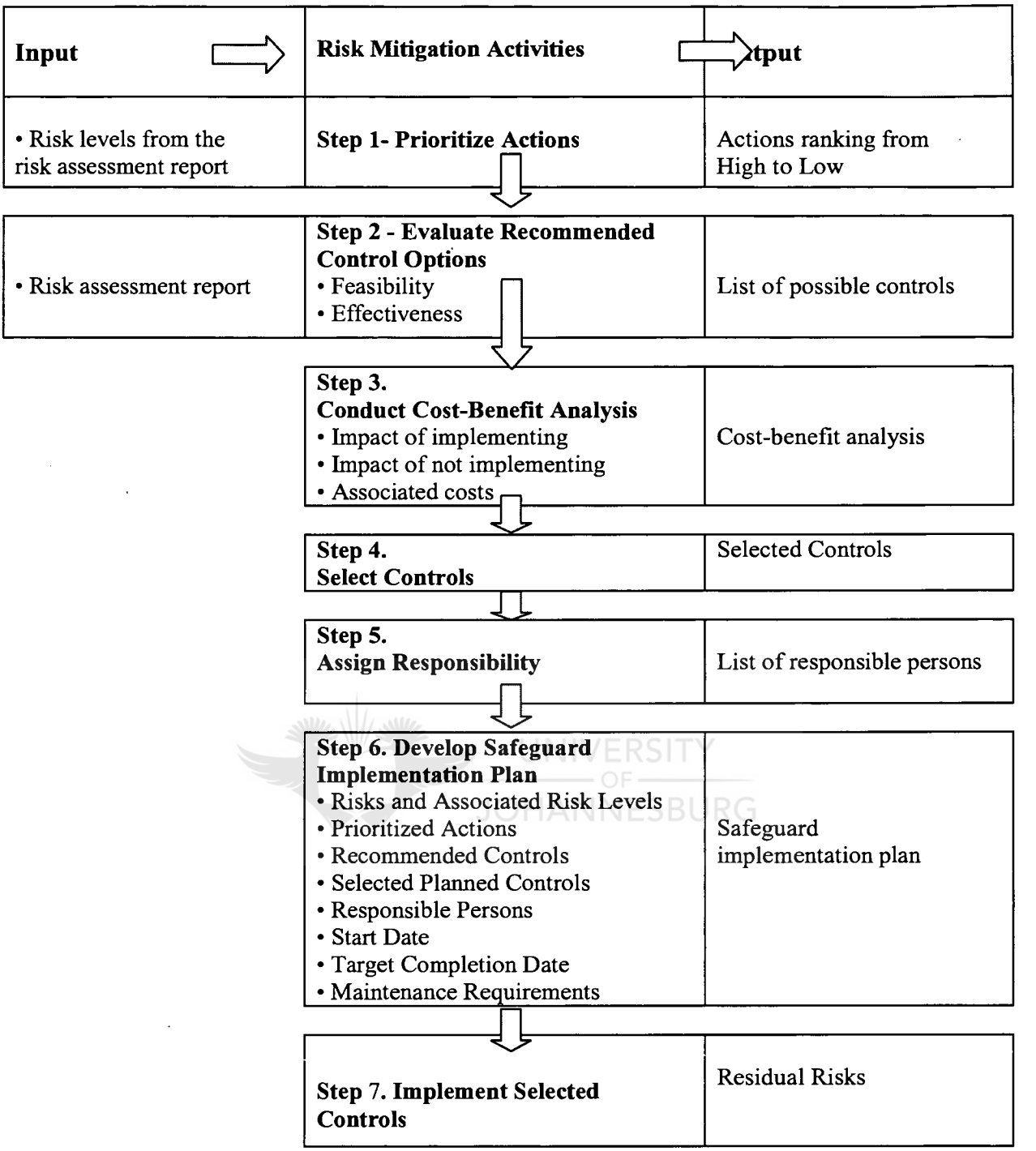

Figure 4.2 - Risk Mitigation Methodology Flowchart [adapted from 1]

4.5. CONTROL CATEGORIES

In implementing recommended controls to mitigate risk an organizations should consider technical, management and operational controls, or a combination of them to maximize the effectiveness of these controls. [1], [4]

This section will address technical, management and operational controls.

4.5.1. Technical Security Controls

Technical security controls involve system architecture, engineering principles and security packages with a mix of hardware, software and firmware. [1], [4]

Technical security controls can be grouped in the following categories:

- Supporting Technical Controls
- Preventive Technical Controls
- Detection and Recovery Technical Controls

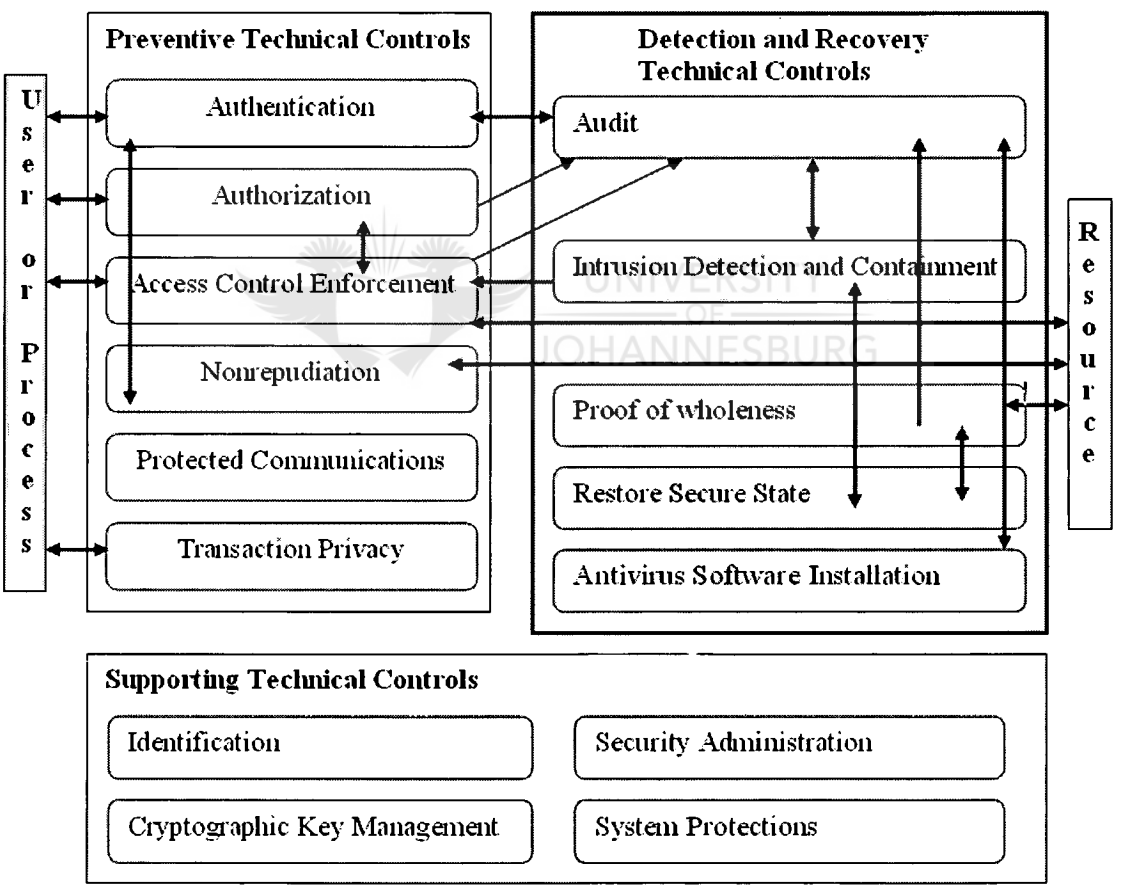

Figure 4.3 – Technical Security Control [adapted from 1]

4.5.1.1. Supporting Technical Controls

These controls are necessary and important to implement other controls. They can be categorized as follows:

- **Identification:** Users, processes and information resources are uniquely identified. This control is also essential to implement other security controls.
- **Cryptographic Key Management:** Key generation, distribution, storage and maintenance should be securely managed.
- **Security Administration:** IT system's security features must be configured to meet the needs of a specific installation.
- **System Protection.** Residual information protection, least privilege, process separation, modularity, layering and minimization of what needs to be trusted are examples of system protection. [1], [4]

4.5.1.2. Preventive Technical Controls

These controls used to prevent security breaches. They are as follows:

- **Authentication:** It is used to verify identity of subject to ensure claimed identity is valid and can have access to system. It includes personal ID number or user name, passwords or pins. Smart cards, tokens, digital certificates and Kerberos are examples of latest authentication methods.

- **Authorization.** The information owner or database administrator determines and assigns rights to personal who can have full or partial access to a system. For example who can update shared files accessed by a group of online users.

- **Access Control Enforcement.** After authorization it is necessary to enforce the defined security policy for data integrity and confidentiality. MAC (Mandatory access control) and DAC (Discretionary access control) are example of these policy-based controls.

- **Non-repudiation.** This control measure is applied at the point of transmission or reception to ensure that senders can not deny sending information and receiver can not receiving it.

- **Protected Communications.** This control ensures the integrity, availability and confidentiality of sensitive and critical information while it is in transit.

- **Transaction Privacy.** Transaction privacy controls protect against loss of privacy with respect to transactions performed by an individual. Secure Sockets Layer and secure shell are examples of this type of control. [1], [4]

4.5.1.3. Detection and Recovery Technical Controls

The following security controls are typically used to detect and recover from a security breaches.

• **Audit.** The auditing monitoring and tracking security related events and system abnormalities are key elements to detect and recover from security breaches.

• **Intrusion Detection and Containment.** It is essential to detect security breaches (e.g., network break-ins, suspicious activities) so that an effective mechanism can be introduced timeously. It is of little use to detect a security breach if no effective response mechanism can be initiated. The intrusion detection and containment control provides these two capabilities.

• **Proof of Wholeness.** The proof-of-wholeness control such as system integrity tool analyzes the system's integrity and irregularities and identifies exposures and potential threats. This control does not prevent violations of security policy but detects violations and helps determine the type of corrective action needed.

• **Restore Secure State Service.** Turns the system to a secure state, after a security breach occurs.

• **Antivirus Software Installation.** Antivirus software should be installed on servers and user workstations to detect, identify, and remove viruses to ensure system and data integrity. [1], [4]

4.5.2. Management Security Controls

Management security controls can be grouped in the following categories:

- Preventive Management Security Controls
- Detection Management Security Controls
- Recovery Management Security Controls

4.5.2.1 Preventive Management Security Controls

These controls include the following:

- Assign security responsibility to ensure that adequate security is provided for the mission-critical IT systems.
- Develop and maintain system security plans to document current controls and address planned controls for IT systems in support of the organization's mission.
- Implement personnel security controls, including separation of duties, least privilege, and user computer access registration and termination.
- Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission. [1], [4]

4.5.2.2 Detection Management Security Controls

Detection management controls are as follows:

- Implement personnel security controls, including personnel clearance, background investigations, and rotation of duties.
- Conduct periodic review of security controls to ensure that the controls are effective
- Perform periodic system audits.
- Conduct ongoing risk management to assess and mitigate risk.
- Authorize IT systems to address and accept residual risk. [1], [4]

4.5.2.3. Recovery Management Security Controls

These controls include the following:

- Offering support continuously and developing, testing, and ensuring that operation plans continuously provide for business resumption and continuity of operations during emergencies or disasters.
- Finding ways of responding to incidents to prepare for recognize, report, and respond to the incident and return the IT system to operational status. [1], [4]

4.5.3. Operational Security Controls

Operational controls are used to correct operational deficiencies that could be exercised by potential threat-sources. To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing operational controls must be clearly defined, documented, and maintained. These operational controls include those presented in Sections 4.4.3.1 and 4.4.3.2 below. [1], [4]

Operational security controls can be grouped in the following categories:

- Preventive Operational Controls.
- Detection Operational Controls

4.5.3.1. Preventive Operational Controls

Preventive operational controls can be categorized as follows:

- Safeguard computing facility (e.g., security guards, site procedures for visitors, electronic badge system, biometrics access control, management and distribution of locks and keys, barriers and fences).
- Protect laptops, personal computers (PC) and workstations.
- Limits access between networks by using firewall and control software viruses.
- Provide regular data and system backups.
- Establish off-site storage and back-up facilities.
- Control data media access and disposal (e.g., physical access control, degaussing method).
- Secure wiring closets that house hubs and cables and limit external data distribution (e.g., use of labeling).

- Protect IT assets from fire damage.
- Provide emergency power source like UPS (uninterruptible power supplies) or on-site power generators.
- Control the humidity and temperature of the computing facility by using air conditioners or heat dispersal. [1], [2], [3], [4]

4.5.3.2. Detection Operational Controls

Detection operational controls include the following:

- Provide physical security (e.g., use of motion detectors, closed-circuit television monitoring, sensors and alarms).
- Ensure environmental security (e.g., use of smoke and fire detectors, sensors and alarms). [1], [2], [3], [4]

4.6. THE COST-BENEFIT ANALYSIS

A Cost-benefit analysis is used to justify the implementation of the controls in terms of cost.

A cost benefit analysis for new controls or enhanced controls encompasses the followings:

- Determining the impact of implementation.
- Determining the impact of non-implementation.
- Estimating the cost of implementation. These may include following;
    - Hardware and software purchases.
    - Maintenance cost.
    - Training cost.
    - Cost for additional policies and procedures.
    - Cost of hiring additional staff to implement proposed policies and procedures.
- Assessing the cost of implementation in terms of system and data criticality to determine the importance to organization.

After all findings, the following rules are used to determine usage of new or enhanced controls:

- If new or enhanced controls cost more than the risk, then look for alternative measures.

- If they don't reduce risk sufficiently, then look for more efficient and different controls.
- If they would reduce risk more than needed, find the less expensive alternatives.
- If they provide enough risk reduction then use it. [1], [2], [3], [4]

4.7. RESIDUAL RISK

In practice, there is no risk free IT system because implemented controls can not reduce the risk level to zero. Residual Risk is the remaining risk after the implementation of new and enhanced controls. Residual risk should be reduced to an acceptable level otherwise; the risk management cycle must be repeated to reduce residual risk to an acceptable level. [1], [4]

The relationship between control implementation and residual risk is shown in Figure 4.4.

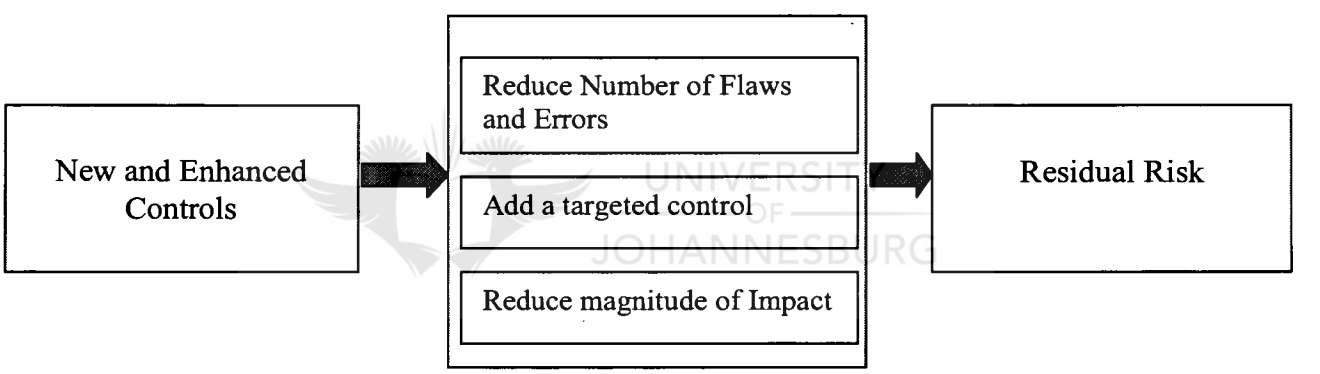

Figure 4.4.Implemented Controls and Residual Risk [adapted from 1]

4.8. CONCLUSION

It has to be emphasized once again that users of IT need not only complain about the threats to organizations, but should be proactive and be in a state of readiness to deal with this threat. Being in a state of readiness means that one has control measures and strategies in place to minimize the adverse impact on organization's resources. It is hoped that if these measures are timeously implemented, they may help to reduce the risks to acceptable level

In the next chapter, the need for an ongoing risk evaluation and assessment and also the factors that will lead to an effective and successful risk management program will be disgusted.

CHAPTER 5

RISK EVALUATION AND ASSESSMENT

"Fear cannot be banished, but it can be calm and without panic; it can be mitigated by reason and evaluation." ***Vannevar Bush.*** *[24]*

5.1. INTRODUCTION

This chapter emphasizes the need for an ongoing risk evaluation and assessment and also the factors that will lead to an effective and successful risk management program.

IT Risk management is an ongoing and evolving process because of changes and new technologies. IT systems continually grow, new computers are added to networks, hardware and software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies will be changed from time to time. These changes create new risks and previously mitigated risks may again become a concern for risk management.

First of all, for successful risk management program, there should be specific schedule for assessing and mitigating risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies.[1]

Secondly a successful risk management program will rely on the following:

a) Senior management's commitment.
b) The full support and participation of the IT team.
c) The talents of the risk assessment team, which must have the expertise to apply the risk assessment methodology and provide cost-effective safeguards that, meet the needs of the organization.

d) The awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization.
e) An ongoing evaluation and assessment of the IT related mission risks.[1], [4], [8]

Thirdly, there are number of principles which can provide a foundation upon which a reliable and consistent structured approach to IT security can be constructed.

These principles may not apply to all systems at all times and are not to be considered as an all inclusive list. They are security principals that can be used in operational environment of all users when the need arises.

The focus of these principles is two-sided i.e. Implementation of technical controls and for non-technical issues, such as policy, procedures and user training.

These principles are:

- Strive for simplicity.
- Minimize the system elements to be trusted.
- Reduce risk to an acceptable level.
- Assume that external systems are insecure.
- Establish a sound security policy as the "foundation" for design.
- Treat security as an integral part of the overall system design.
- Clearly delineate the physical and logical security boundaries governed by associated security policies.
- Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
- Implement layered security (Ensure no single point of vulnerability).
- Implement tailored system security measures to meet organizational security goals.
- Design and operate an IT system to limit vulnerability and to be resilient in response.
- Implement security through a combination of measures distributed physically and logically.

- Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
- Limit or contain vulnerabilities.
- Formulate security measures to address multiple overlapping information domains.
- Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
- Use boundary mechanisms to separate computing systems and network infrastructures.
- Where possible, base security on open standards for portability and interoperability.
- Use common language in developing security requirements.
- Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
- Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
- Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
- Use unique identities to ensure accountability.
- Implement least privilege.
- Do not implement unnecessary security mechanisms.
- Protect information while being processed, in transit, and in storage.
- Strive for operational ease of use.
- Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
- Consider custom products to achieve adequate security.
- Ensure proper security in the shutdown or disposal of a system.
- Protect against all likely classes of "attacks."
- Identify and prevent common errors and vulnerabilities.
- Ensure that developers are trained in how to develop secure software.[2]

5.2. CONCLUSION

This chapter has shown that because of changes happening in the global marketplace, IT has become valuable business assets that need to be protected. Organizations and government agencies for successful business operations are therefore required to have comprehensive well designed, and reliable information security programs. These efforts are designed to address many aspects of information security at many levels.

These efforts must be seen as an ongoing and evolving process because of changes and new technologies.

To aid in designing a secure information system, this chapter has included principles derived from a number of documents with the hope that they can contribute to improved IT security in any organization. From users to system administrator and managers, everyone should have a basic understanding of these security principles governing the system they are using, maintaining or designing and developing.

CHAPTER 6

CASE STUDY

"It is matter of choice." **Esquire**

6.1. COMPANY OVERVIEW AND INTRODUCTION

Esquire Technologies Holdings is a premier distributor of computer components, desktops, notebooks and peripherals in Southern Africa.

Esquire distributes world-renowned brands to resellers, distributors, system integrators and builders in the computer industry in South Africa, Mozambique, Namibia, Swaziland, Zimbabwe and Zambia.

Esquire's strives to deliver global Tier 1 technology products at the best price in the fastest turn-around time to local markets

Esquire is a truly South African owned black empowerment IT Company committed to the upliftment of its staff and the broader South African community.

Leading brands

Esquire is a distributor in South Africa for global brands, including:

- Altec Lansing speaker systems
- BenQ Joybooks, MP3 players K/B mouse and CDR media
- CTX monitors, projectors & optical drives
- ECS motherboards and notebooks
- Kingmax memory products
- KWorld Digital TV products for PCs
- Manhattan range of PC components and peripherals
- Micronet networking products
- Prolink graphic & multimedia adaptors
- Sapphire graphic card solutions

- TEAC optical drives
- Xitel multimedia products

Key Global Relationship

Esquire has several key global value chain relationships, including

- Intel Premier Provider.
- Microsoft Tier 1 Managed System Builder.
- First Premier Partner (System Builder) for Computer Associates E-Trust Antivirus software in South Africa.
- Western Digital Select Golden Partner.
- Premier Partner for Seagate.

Location

Esquire Technologies' head office is based in Samrand, Gauteng, which is accessible from Pretoria, Johannesburg and Johannesburg International Airport.

The company has branches in Midrand, Durban, Cape Town, and Port Elizabeth. The sales, warehouse and production facilities, comprising approximately 6000 square metres, is situated at the head office and provides for service, product training, sales training, product presentations, and product display. Esquire's strong sales team handles enquiries from all parts of southern Africa.

Esquire is an equal opportunities employer and has a staff contingent of over 120 staff members at its head offices and regional branches.

Product Range

Esquire's product range includes:

- Esquire branded PC range from entry level, mid range to high end and servers based on the Intel and AMD platforms
- Esquire range of Notebooks from entry level, mid range to high end based on the Intel and AMD platforms
- Components Motherboards - Processors Memory - Processor Fans
- USB Memory Flash Drives - Hard Drives - VGA Cards

- Floppy Drives – CD-Rom Drives - DVDs - Sound Cards
- Speakers - Mouse - UPS - Software
- Server Cases - Digital Cameras - Input Devices - Monitors
- Fax Modems - Printers - Video Adaptors

Xpress Warehouse

Esquire Technologies was the first computer distributor in southern Africa to open a retail type store on 18th March 2005, called Xpress Warehouse, aimed exclusively at resellers. The warehouse "retail" concept will go a long way to expedite the sales' cycle and introduce a more exciting purchasing experience for Esquire's resellers. Customers enter the Xpress Warehouse, select a product off the shelf and pay for it at the counter. Trained sales representatives on the floor and a help booth are on hand to lend advice and assistance.

Technical Services

Esquire has a team of professional technical staff that all receive ongoing hands-on training to ensure customers of optimal service. In addition, Esquire has a highly trained team focusing on Research and Development and control assurance processes.

Esquire offers a comprehensive range of technical support and services, which includes:

Complete System Assembly Service - customized "build to order" systems that meet specific user needs, enabling resellers to provide added value to customers.

Repairs – Esquire has a qualified engineer who supervises workshop repairs and technical enquiries.

Technical Support – Esquire's technical support personnel help customers with installation, set up, integration, as well as field problems. They are also available for demonstrations, product training and seminars.

Marketing Support – Esquire provides customers with promotional items such as product literature, brochures, and evaluation units to aid in closing sales. Esquire works closely with customers on all bids, tenders and quotations, providing not only competitive prices, but also the best all-around solution.

ESQUIRE Vision

To become one of the most admired and dynamic Black Empowered IT distribution companies and the distributor of choice in Africa in the foreseeable future that operates on global principles to deliver best-of-breed products to the benefit of all stakeholders.

ESQUIRE Mission

To source and distribute best-of-breed, global computer hardware and peripherals to its customers in southern Africa, while ensuring high levels of availability and personal service and support at competitive pricing.

ESQUIRE Management Team

Head Office:

CEO: Mahomed Cassim

Managing Director: Asgar Mahomed

Group Sales and Marketing Director: Mahomed Cassim

Group Financial Manager: Hoosein Saleh-Mohamed

Group Human Resource Manager: Verénice du Toit

Midrand:

Branch Manager: Jacques Wynbergen

Channel Account Manager: Kevin Botha

Channel Account Manager: Ihsaan Jaffer

Channel Account Manager: Osman Ali

Product Manager: Juan Beukes

Product Manager: Zane De Beer

Cape Town:

Branch Manager: Brandt Olivier

Durban:

Branch Manager: Jeni Nel

Port Elizabeth:

Branch Manager: Jan Korb

6.2. RISK MANAGEMENT OF ESQUIRE TECHNOLOGIES:

Esquire Technologies has one main headquarter located in Midrand and four branches in Capetown, Durban and Port Elizabeth

There are 75 computers in Midrand and 50 of them are connected to the Fincon File server while 10 computers from each of the branches are connected to file server. The current Esquire network is shown in figure 6.2.

Like all the other organizations and businesses, Esquire Technologies uses an IT system to operate its business.

They know the importance of having a risk management strategy to protect its business since the IT system is vulnerable to various attacks resulting in losses for organizations as discussed in chapter 1 and also shown in figure 1.1 and chapter 2 section 2.1- Importance of risk management

They have developed a safeguard implementation plan based on the following information: responsible teams and staff, risk levels, selected planned controls and prioritized actions as shown in the figure 4.2 – Risk Mitigation Methodology flowchart to address the greatest risks and strive for sufficient mitigation at the lowest cost with minimal impact on other mission capabilities.

To do this, they raised awareness of these risks, as well as corresponding the policies, practices and procedures available to respond to these risks and to encourage appropriate safeguards. Table 3.1 on risk assessment presents an overview of many of today's common human threats, methods used and their possible reasons which Esquire Technologies have also integrated in their strategy. [27]

Esquire technologies is in the process of implementing most of the technical, management and operational controls that are discussed in the risk mitigating chapter 4 section 4.5.1.Technical Security Controls, 4.5.2.Management Security Controls and

4.5.3.Operational security Controls. They also follow all the latest developments in IT risk magement.

Following are some technical, management and operational security measures Esquire Technologies is taking which are in line with risk mitigating chapter 4 section 4.5.1.Technical Security Controls, 4.5.2.Management Security Controls and 4.5.3.Operational security Controls. :

- Esquire uses security-hardened PC configuration with features such as antivirus and firewall applications, VPN (Virtual Private Network) clients for remote access and file encryption to protect information.

- Esquire uses the latest operating system software like windows 2000, Windows XP professional for workstations and Windows Small Business Server 2003 because it is a reliable operating system and easy-to-use network tools including system back up, fax service, network security, and virus protection.

- System administrator creates and controls accounts for users of Fincon Accounting software on the server machine. Figure 6.1 is a view of Fincon Accounting software.

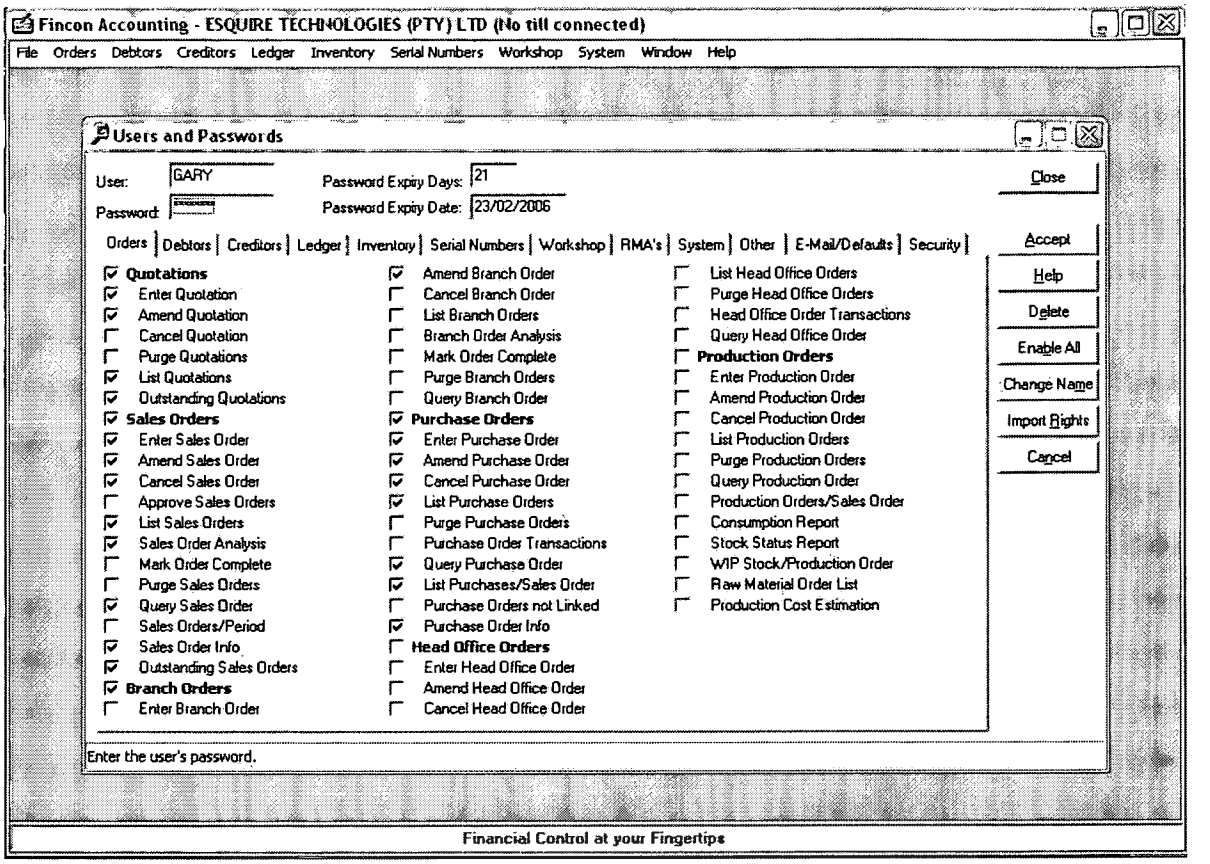

Figure 6.1 – A view of Fincon Accounting Software

- All the information is kept in the Esquire Fincon Server and the off-site back up server is located in another building.
- Trend Micro Office Scan Antivirus software is installed on servers and user workstations to detect, identify, and remove viruses to ensure system and data integrity.
- To prevent unauthorized access to network and computers they use Basilisk Firewall software.
- They train all the staff that uses workstations and Fincon Accounting Software.
- Esquire Technologies is currently using the network as shown in figure 6.2.They decided to upgrade it to more secure and faster network as shown in figure 6.3.

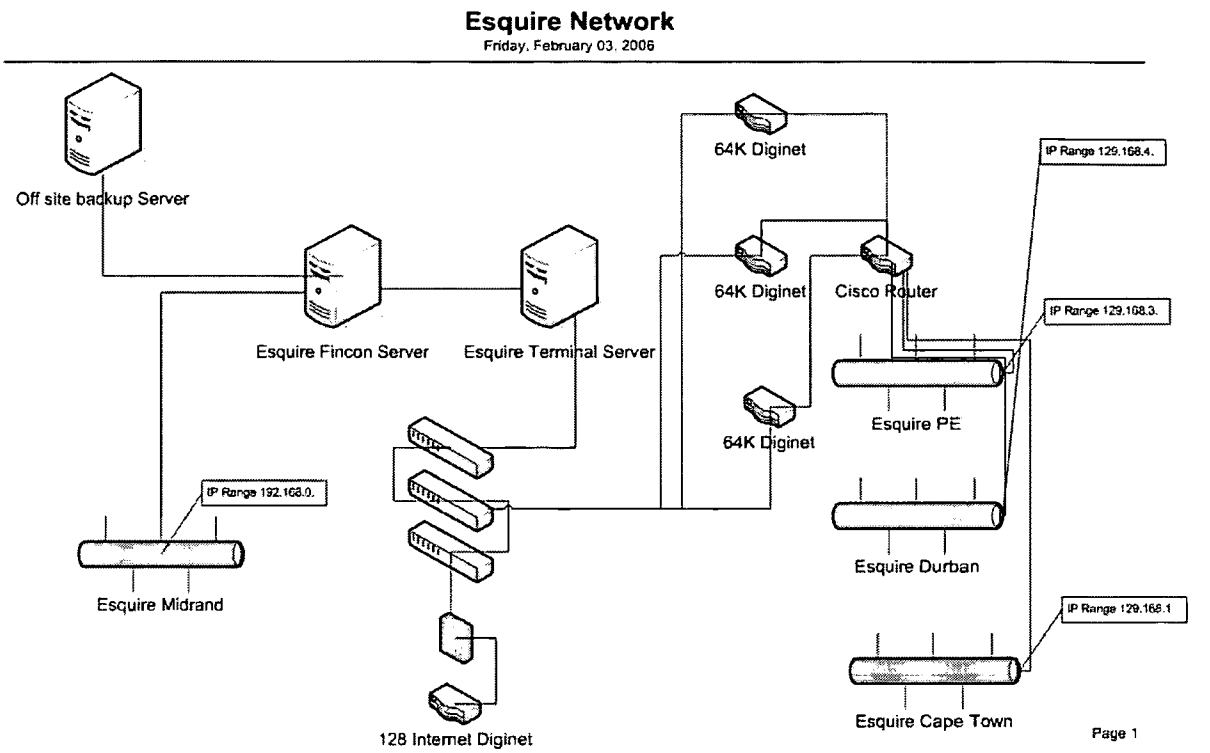

Figure 6.2 - Esquire Network

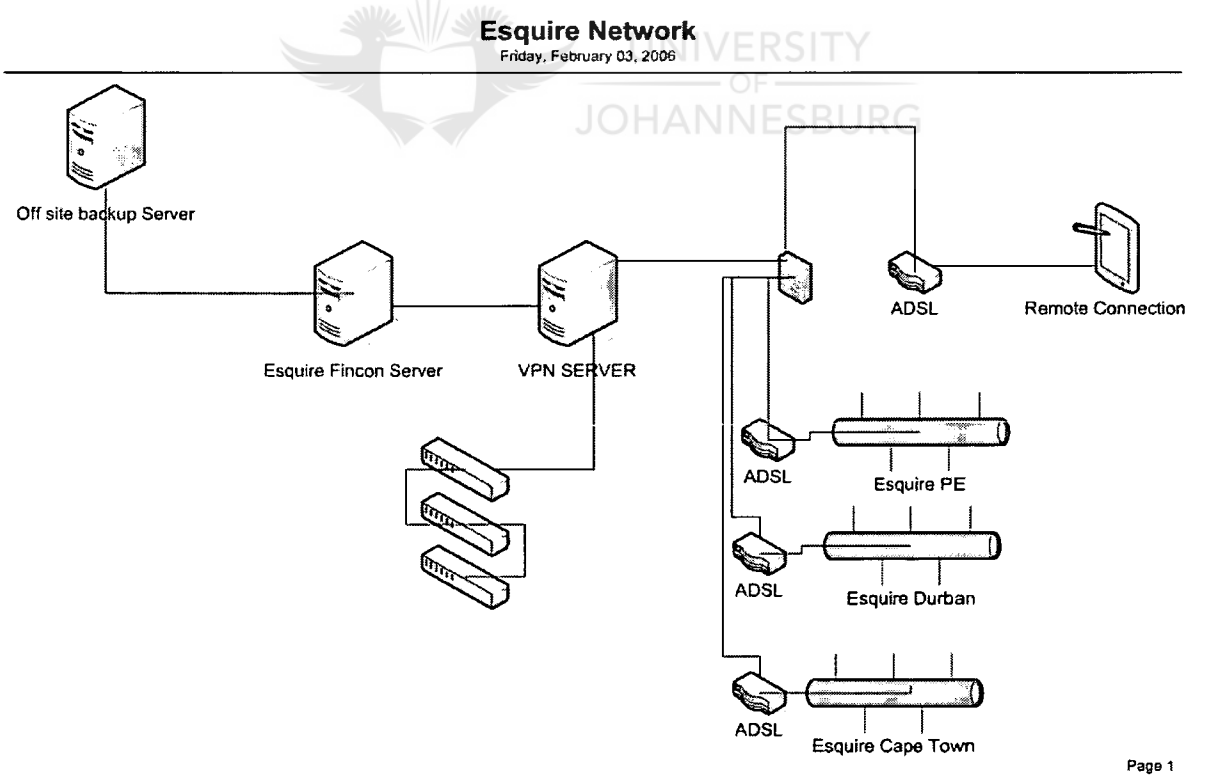

Figure 6.3 – New Esquire Network

Following are some security incidents, as discussed in Chapter 4 section 4.5.1.3. Detection and Recovery Technical Controls, faced by Esquire and solutions used by Esquire:

Information theft.

One ex-employee was caught copying valuable customer information to disk and this was causing loss of clients for the company because 80% of revenue is generated by 20% of these main clients.

To prevent this, database file properties are set to list content only on the server machine. When someone tries to copy a file then the message will be automatically relayed to the system administrator to alert him or her of the intrusion to the system.

Web site defacement

Once someone defaced the Esquire web site. Then Esquire contacted the company that host the Esquire web site and they corrected the problem in one hour. [27]

6.3. CONCLUSION

Esquire Technologies with a history that stretches back to the late nineties, is a leading South African distributor of computer components, desktops, notebooks and peripherals which operates its business fully aware of risks involved in this business, and has therefore put in place a risk management strategy to ensure the smooth running of its business by implementing technical, management and operational security controls.

The use of latest hardware, software, well trained and equipped personnel are indeed signs of a company to keep abreast of challenges of the modern world. It should be clear from the way they operate the business that they are intending to follow the latest developments in risk management.

CHAPTER 7

CONCLUSION AND RECOMMENDATION

"It is how you deal with failure that determines how you achieve success." ***David Feherty*** *[25]*

7.1. CONCLUSION

This report has shown that computer based information systems have become of critical importance to governments, organizations and individual users for stable and efficient national economies and international trade and in social, cultural and political life. This therefore calls for social efforts to protect and foster confidence in them.

This is because information systems and networks and their worldwide usage have been accompanied by new and increasing risks, and are subject to threats from various means of unauthorized access, such as misuse, misappropriation, alteration, malicious code transmission, denial of service or destruction.

Therefore this report calls for a need to raise awareness of risks to information systems and networks and of the policies, practices, measures and procedures available to respond these risks.

However, this report recognizes that absolute security is an unrealistic goal. The aim of risk management is to reduce the risk to an acceptable level. The more knowledge there is about the causes and consequences of computer security breaches, as well as the way organizations address these issues, the more likely it is that computer security will improve. The challenge to users of computer systems and networks is to plan carefully from the earliest stages and to integrate risk management into the five SDLC phases to make security awareness a way of life within an organization and for all users to have access to easily understood guidance.

Esquire Technologies, our case study, have put in place some management, operational and technical security controls that can be use in operational environment when the need arises. It is however clear that they still face a critical task of strengthening security to meet their developmental objectives. Each sphere of the company should be properly positioned to apply the risk assessment methodology and provide cost-effective safeguards. There is also a need for them to have a realistic integrated security plan and material and human resources, as well as the management and operational systems to implement security policy. They need to address identified serious capacity constrains arising from a shortage of properly qualified managers and technical personnel, create awareness and cooperation among its members who must follow procedures and implement principles which can provide a foundation upon which a reliable and consistent structured approach to IT security can be constructed. These principles, as discussed in chapter 5 – Risk Evaluation and assessment focus on implementation of technical and non-technical issues such as policy, procedures and user training.

This report, however, does not suggest that any unique solution exists for security, but rather provides a framework of principles to promote better understanding of how participants may benefit from, and contribute to the development of a culture of security.

Self-protection, while essential, is not sufficient to make information systems and networks safe. The rule of law must also be enforced. National governments should examine their current statutes to determine whether they are sufficient to combat the kinds of crimes discussed in this report, where gaps exist, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these crimes.

This report recognizes risk management as a fundamental management responsibility which requires the support and involvement of senior management. The control measures outlined in this report can be used to mitigate for the better protection of critical information and the IT systems that process, store and carry information.

This report also recognizes the need for an ongoing risk evaluation and assessment and also the factors that will lead to an effective and successful risk management program. As

changes in IT systems grow, new computers being added to the networks and hardware and software applications being replaced or updated there is need for management to review security measures from time to time to foster international cooperation and better and quick response to new risks and to ensure that previously mitigated risks do not become a concern again. This has specifically been illustrated in the case study presented in Chapter 6.

7.2. RECOMMENDATION

It should be noted that IT is a subset of the broader knowledge domain of information and communication technologies (ICTs) which is the convergence of Information Technology, Telecommunications and Data Networking Technologies into a single technology.

In light of this, one would recommend that future research should cover the whole spectrum of Risk Management in ICTs. In particular, it could be about Risk Management in E-Commerce or Risk Management in Internet Banking. Since the information has become as valuable as money, it has created new areas for crime as most countries are becoming cashless societies, dependent on internet, electronic banking systems, E-Commerce, credit cards and smart cards.

REFERENCES:

1. National Institute of Standards and Technology (NIST) Technology Administration. U.S. Department of Commerce. Special Publication 800–30 Risk Management Guide for Information technology Systems. By Gary Stoneburner, Alice Gougen and Alexis Feringa , July 2002

2. National Institute of Standards and Technology (NIST) Technology Administration. U.S. Department of Commerce. Special Publication 800–27. Engineering principles for Information Technology Security. By Gary Stoneburner, Clark Hayden and Alexis Feringa, June 2001

3. National Institute of Standards and Technology (NIST) Technology Administration. U.S. Department of Commerce. Special Publication 800–14 Generally Accepted principles and practices for Securing Information Technology Systems. By Marianne Swanson and Barbara Guttman, September 1996.

4. National Institute of Standards and Technology (NIST) Technology Administration. U.S. Department of Commerce. Special Publication 800–12 An Introduction to Computer Security: The Nist handbook.

5. OECD Guidelines for the Security of Information Systems and Networks. Towards the Culture of Security. By OECD (Organization for Economic Co-Operation and Development.) 2002.

6. Risk Management of Digital Information by Gregory W.Lawrence, William R.Kehoe, Oya Y. Rieger, William H. Walters, Anne R. Kenney, June 2000.

7. Risk Management and Business Continuity Overview and Perspectives – White Paper by Dennis Wenk (Hitachi data Systems) , February 2005

8. Reducing the Risk by Allyson Klein.
(Initiative marketing manager for Intel Corp.'s Enterprise Platform Group). http://www.computeruser.com/articles/2409,1,3,1,0901,05.html, September 2005

9. Cyber crime impedes regional trade – by Alari Alare in Johannesburg / Business news / date: 7 October 2005

10. Is Your Business Safe From Internet Security Threats? July 11, 2005 / By Peter Alexander

11. A Case Study of in Industrial Risk Management by P.J. Raubenheimer July 2000 – Rand Afrikaans University

12. 2005 CSI / FBI Computer Crime and Security Survey.

13. 2004 CSI / FBI Computer Crime and Security Survey.

14. Computer Crime : Challenges of new technology Published in Nedbank ISS Crime index volume 3 1999 Number 4, July- August

15. http://www.internetworldstats.com/stats.htm / date: 31 December 2005

16. www.polity.org.za Online News - Examining the real cost of virtual crime by Irma Venter / Date: 10 October 2005

17. International Fraud Trends: South Africa at risk1 by Lala Camerer – Published in African Security Review Vol 6 No 2, 1997

18. Threats to Computer systems

http://rf-web.tamu.edu/security/secguide/V1comput/Threats.htm / date: 31 December 2006

19. www.wiley.co.uk/college/turban/glossary.html

20. www.ballyclarehigh.co.uk/garden91/Glossary_finalRW.htm

21. en.wikipedia.org/wiki/Computer_crime date: 21 January 2006

22. http://www.wisdomquotes.com/cat_risk.html date : 21 January 2006

23. http://www.brainyquote.com/quotes/authors/b/bill_nelson.html date: 21 January 2006

24. http://open-mind.org/SP/Quotes.htm date: 21 January 2006

25. http://quotations.about.com/cs/inspirationquotes/a/RiskTaking8.htm date: 31 January 2005

26. Understanding And Managing Risk – Borland white paper – March 2005

27. Esquire Technologies, web: www.esquire.co.za, address: Unit No 6 N1 Industrial Park Komosdal Ext 11 Samrand / Gauteng / South Africa