CHAPTER SIX:
IMPLEMENTING INFORMATION SECURITY GOVERNANCE

6.1 Structure of chapter

This chapter aims at providing directors and top management with guidance when wanting to implement information security governance within their organisations. It will illuminate what is expected of directors and top management in order to effectively discharge their responsibility of due diligence.

The researcher proposes a seven-step plan for the successful implementation of information security governance within an organisation. It is expected of the board and top management to be involved in every step of this process. Furthermore, their commitment to, and support of the implementation of information security governance must be clearly visible. It is contended by the researcher that a director will be able to discharge his duty of due diligence if he can indicate to the court that: (i) the suggested framework was implemented and executed effectively within his organisation; (ii) he has insight into what every stage of the implementation process involves; and (iii) he played a central role in each step.

Outline of chapter:

Part 2: briefly highlights the motivation behind, and importance of the actual implementation of information security governance, thereby setting the tone for the rest of the chapter; and

Part 3: sets forth a useable framework for the implementation of information security governance within the organisation. This part is subdivided into seven subsections, each representative of a step the organisation must take to effectively implement and integrate information security governance into the organisation.

Explanation of how part 3 should be read:

The researcher provides the reader with: (i) an objective; (ii) outcome; and where necessary, (iii) roadmap, to each step. Therefor, a very analytical approach is taken, with each step being dissected and broken down into its bare essential components. This will enable the reader to gain a better understanding of what each step entails, while simultaneously ensuring that the reader does not loose his/her way half way through the process.

It is concluded that the effective implementation of information security governance is dependent on two critical success factors. Firstly, the concept of information security governance must be embraced. [1] Therefor, top management must be committed to this discipline, and this commitment must cascade down to lower level employees. Ultimately this will result in a culture of security being fostered within the organisation. Secondly, information security must effectively be executed and implemented within the organisation. [2]

6.2 Introduction

Organisations might feel bewildered by the plethora of seemingly disjointed information security components that they must consider when wanting to implement information security governance within their organisation. To aid directors and top management in the integration of this governance discipline this chapter presents them with a useable framework through which they can implement and maintain information security governance within their respective organisations. When reading this chapter the reader must be mindful of the fact that the proposed framework takes a life cycle approach, with each phase acting as a continuation of the previous phase and a predecessor of the next.

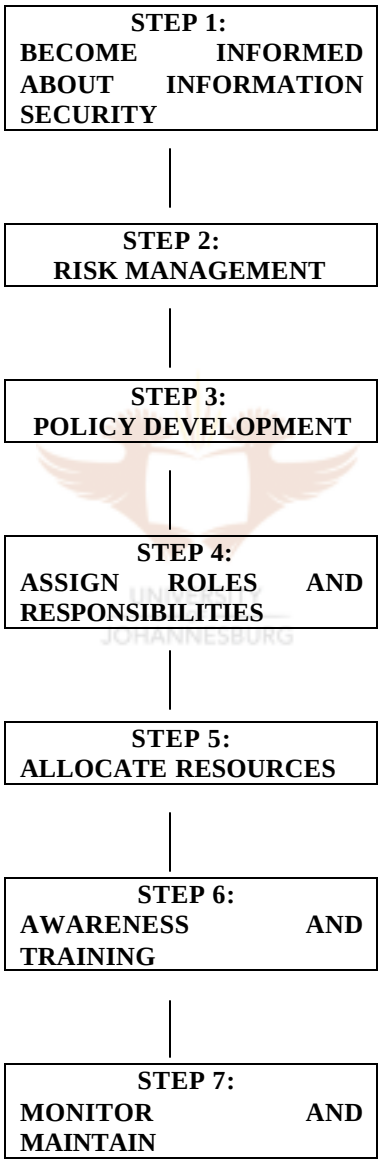
---

1 Jenkins "Organizational IT security theory and practices: and never the twain shall meet?" (last visited 27 February 2003) http://www.sans.org/rr/securitybasics/IT_sec2.php 1.

2 ibid.

6.3 Managing information assets – explanation of the framework

The following framework provides directors and top management with a description of what is expected of them when attempting to implement information security governance in order to protect the organisation's information assets.



Tudor[3] argues that if any one of these domains is neglected, it will result in vulnerabilities being exploited, not only in that specific domain, but also in the organisation as a whole, as all of these domains function interdependent of one-another. A deficiency in one will directly impact on the other domains. One must be mindful of the fact that these steps do not necessarily take place in the chronological order as depicted above. Some of these steps may transpire alongside one-another.

STEP 1: BECOME INFORMED ABOUT INFORMATION SECURITY

OBJECTIVES OF STEP 1:

(i) Educate directors and top management on what the discipline information security governance entails;
(ii) Gain their support and commitment to this discipline; and
(iii) Have top management support and commitment cascade down to lower levels of the organisation.

6.3.1.1 Introduction

Boards need to "lead by example". Therefor it is first and foremost required of them to educate themselves on what the discipline of information security governance entails.[4] At present there exists a significant lack of understanding amongst top management regarding information security-related issues.[5] Yet, as have been observed in chapter four the ultimate responsibility for information security governance is vested in the board of directors. The board will therefor be held accountable for the governance of information

3 Tudor *Information Security Architecture* (2001) xiii.
4 Roberts *Computer Security Policy* (1990) 123.
5 Khan "Info Sec Africa formed" (last visited 18 April 2002) http://www.itweb.co.za 1.

security, regardless of their knowledge or lack thereof on the subject-matter.[6] Consequently the onus rests on the board to ensure that: (i) they understand what this discipline entails; (ii) what is expected of them; and (iii) what they can be held liable for.[7]

This step would imply that they need to: (i) acknowledge the importance of information as an asset to the organisation; and (ii) be involved in the development and execution of the discipline. [8]

6.3.1.2 Acknowledge the importance of information assets

As observed earlier, information is one of the most important assets over which an organisation may possess. It does not merely support the organisation, but also enables it. Furthermore, there is a direct correlation between the effectiveness of the board, and the information it receives.[9] It is therefor of critical importance to protect the information assets of the organisation in order to directly and indirectly protect the business strategy of the organisation and gain a sustainable competitive advantage. [10]

Organisations have their own specific requirements for the protection of their information assets. However, in general there are three common "attributes" of information that all organisations strive to protect, namely: [11]

(i) **Integrity** - guard against unauthorised modification or corruption of information; [12]

---

6 IT Governance Institute "Infomation security governance" (last visited 24 July 2002) http://IT governance.org 11.

7 (n 4) 118.

8 United States General Accounting Office, Accounting and Information Management Division *Information Security Management: Learning from leading organisations* GAO/AMD-98-68 (May 1998) 22.

9 Wixley and Everingham *Corporate Governance* (2003) 79.

10 (n 8) 22.

11 Peltier *Information Security Risk Analysis* (2001) 4-5. For a more comprehensive discussion of these three pillars, as well as an additional three see chapter two.

12 Appelgate, McFarlan and McKenney *Corporate Information Systems Management* (1999) 154.

(ii) **Confidentiality** - protects information against unauthorised, intentional or accidental disclosure;[13] and

(iii) **Availability** - ensures that information is at the disposal of authorised users when needed. [14]

6.3.1.3 Top management support and commitment

The commitment and support of top-level management is of crucial importance.[15] If directors and top management do not support the information security governance discipline, lower levels of the organisation will not take it seriously.[16]

OUTCOMES DELIVERED BY STEP 1:

Primary and secondary role-players:

(i) Gain a comprehensive understanding of the discipline information security governance; [17]

(ii) Are involved throughout the whole information security governance process;[18] and

(iii) Are committed to the process. [19]

---

13 (n 3) 1.
14 (n 3) 2.
15 Bowden, Lane and Martin *Triple Bottom Line Risk Management* (2001) 41.
16 (n 8) 22-23.
17 (n 8) 23.
18 ibid.
19 ibid.

STEP 2: RISK MANAGEMENT

OBJECTIVES OF STEP 2:

Determine the radius of risk to information security within the organisation by enabling directors and top management to:

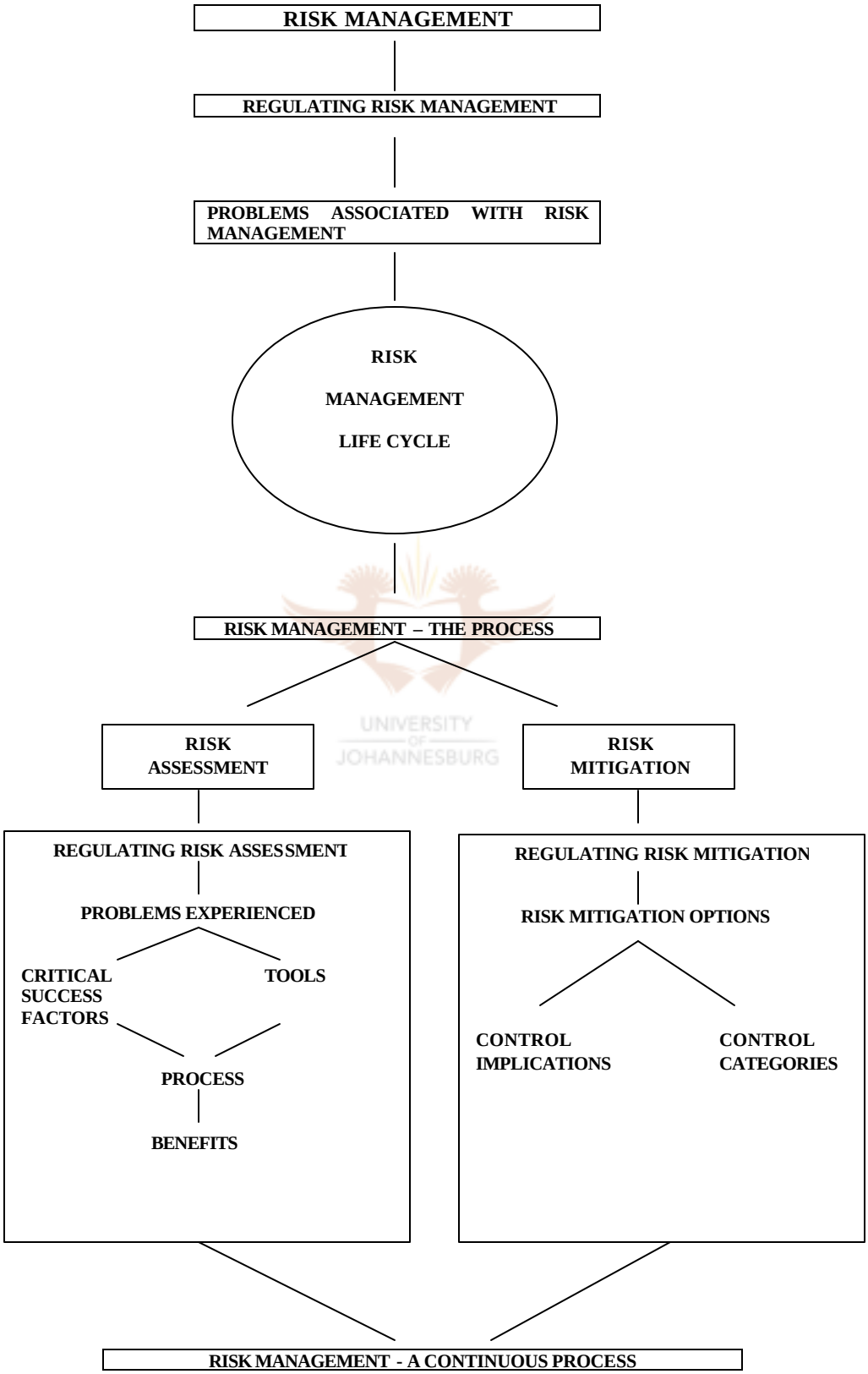
(i) Appreciate the general concept of risk in relation to the organisation;

(ii) Understand the standard risk assessment methodology, together with its advantages and disadvantages;

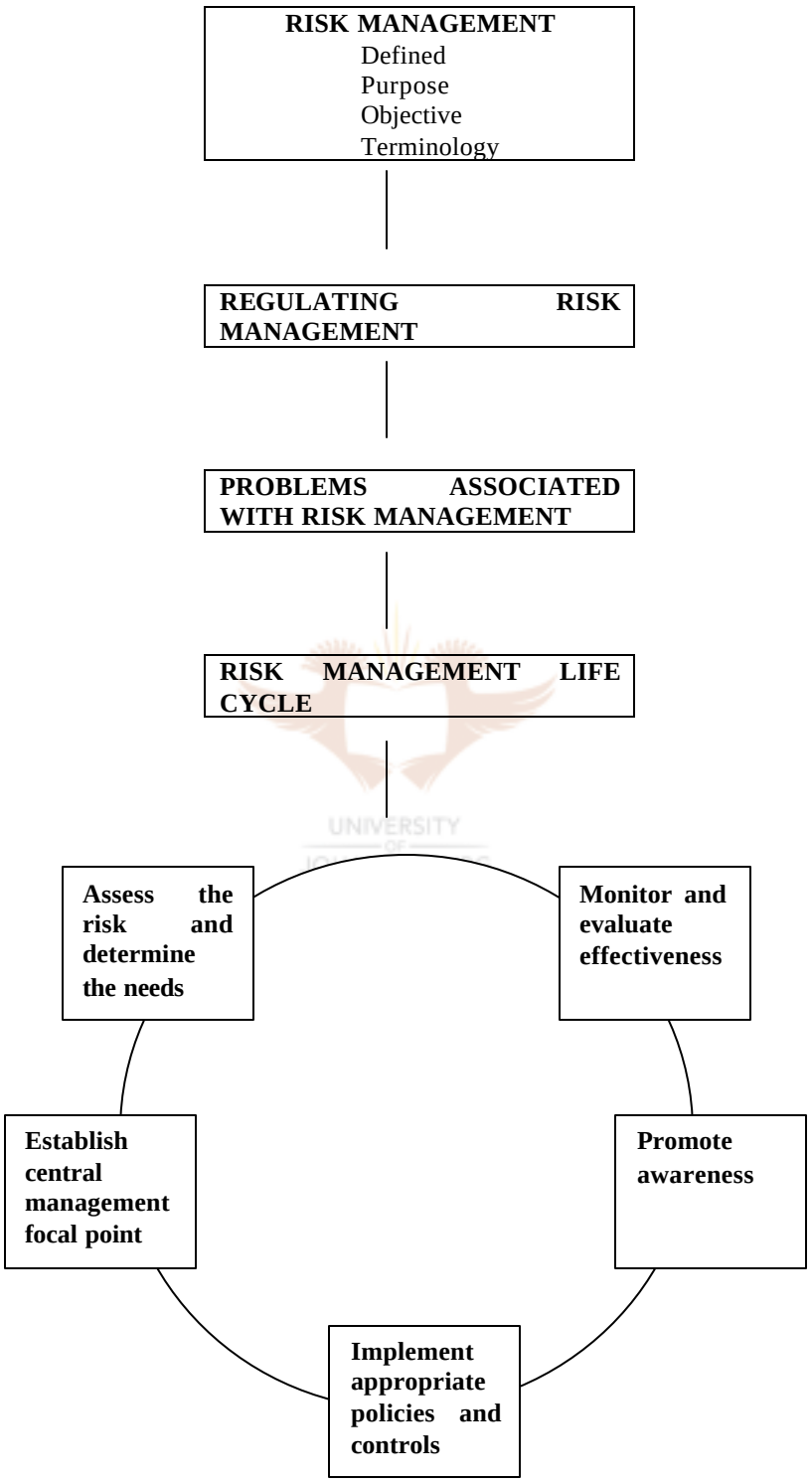
(iii) Gain insight into what risk mitigation entails; and

(iv) Be equipped to implement a risk management process that will demonstrate commitment and due diligence to shareholders.

FRAMEWORK OF STEP 2:



ROADMAP TO RISK MANAGEMENT:



6.3.2 Information security risk management for company executives

6.3.2.1 Introduction

The concept of risk is not foreign to the business world, [20] it has evolved over thousands of years. [21] Uncertainty represents the negative side of risk, whereas opportunity is equated to the positive side of risk. Therefor "success in business and in life results from exploiting opportunities but managing risks."[22]

The need for risk management may be illustrated by the following two principles:[23] firstly, if the risks of the organisation are effectively managed the organisation will better be able to fulfill its mission, goals and objectives, therefor risk management will enhance the organisation's value.[24] Secondly, the regulatory environment within which the organisation functions demands of organisations to have an effective risk management systems in place, not only in the financial arena, but also in other spectrums of the organisation. [25]

Recent corporate failures highlight the importance of an effective risk management process. Various high-profile companies have fallen prey to financial and accounting scandals.[26] This is in part due to the lack of accurate, timely and complete information being available to top management, and in part due to dishonest, greedy or simply

---

20 Briers *A New Language of Risk* (2002) 239.

21 Briers (n 20) 239 observes "…from fear of the unknown to uncertainty and risk, the concept has always been a fundamental part of human existence..." .

22 (n 9) 78.

23 Smullen *Risk Management for Company Executives* (2000) 8.

24 (n 23) 131.

25 Bowden, Lane and Martin (n 15) 5 observe that "(t)he commercial and legal consequences of failure to adequately identify, understand and manage risk can be substantial. Increasingly, due diligence clauses in legal statutes, corporate governance requirements, and corporate social responsibility principles require companies to identify and manage their risks."

26 Amongst these organisations are Enron, Regal; WorldCom and Xerox, all US companies experiencing accounting reporting problems. Williams "IT management: how IT governance can help stop scandal" (last visited 26 July 2002) http://www.ComputerWeekly.com 1.

incompetent directors.[27] Although risk management can not directly guard against the latter, it will contribute to ensure that reliable information is timeously available within the organisation. Irrespective of what the motivation behind a risk or threat materialising is, the result inevitably remains the same – an all but complete loss of shareholder and customer confidence, and irreparable damage to the reputation of the organisation. [28]

At present information may be viewed as being "the life force of the organization."[29] It is one of the most valuable assets over which an organisation may possess. [30] This is true because information supports and enables the organisation's mission, goals and objectives. [31] It furthermore enables top management to make informed decisions, and forms an integral part of the organisation as a whole. [32] It is therefor understandable that organisations would want to safeguard this asset as effectively as possible. Consequently, a new subdiscipline of risk management has evolved in the form of information security risk management.

Top management may however contend that information security risk management represents a specialised field that is too complex and technical for them to fully comprehend, and as a result most activities concerning this issue are left to be dealt with by technical experts. [33] Such an approach is flawed: how does top management expect to make informed decisions if they do not know which questions to ask, or understand which risks the organisation are faced with? How can they even begin to formulate a plan to reduce or mitigate these risks if they do not understand the very nature of the risks involved? [34] The King II report anticipated such an abdication of responsibilities and provides in no uncertain terms that the ultimate responsibility for risk management is

---

27 ibid.
28 ibid.
29 Fitz-endz *The E-Aligned Enterprise* (2001) 55.
30 (n 23) 93.
31 ibid.
32 ibid.
33 Williams "IT management: how IT governance can help stop scandal" (last visited 26 July 2002) http://wwwComputerWeekly.com 2.
34 (n 12) 156.

vested in the board. [35] It furthermore places the board under the obligation to educate itself on the risk management process. [36]

The objective of this discussion is therefor to illuminate the process of risk management, thereby aiding directors and top management in discharging their responsibilities.

6.2.3.2 Purpose of risk management

> "The aim of a risk management system is to provide a framework within which business risks are systematically and proactively identified, assessed, managed, and monitored across the full spectrum. Such a system offers a tool to assist company directors and managers to demonstrate due diligence in the execution of their responsibilities."[37]

The ultimate goal of any risk management program is therefor to identify significant risks that may influence the organisation negatively in achieving its mission, goals and objectives,[38] and reduce these risks to levels that are deemed to be acceptable.[39]

35 King Committee *King II Report on Corporate Governance 2002* (2002) 73-85.
36 (n 35) 79.
37 (n 15) 116-117.
38 Every organisation has as its main mission, goal and objective to: (i) make a profit; (ii) provide quality services and products; (iii) be as efficient and productive as possible; and (iv) stay within the boundaries of the law, while achieving a sustainable competitive advantage.
39 (n 15) 15.

6.3.2.3 Objectives of risk management

Risk management has as its objective to:

(i) Enable top management to make informed decisions based on reliable, current and accurate information; [40]

(ii) Ensure better security for the organisation as a whole, and specifically for its information assets; [41]

(iii) Display management's performance of due diligence in running the organisation; [42] and

(iv) Ensure compliance with applicable laws, regulations and industry standards. [43]

6.3.2.4 Risk-related terminology

Confusion exists regarding risk-related terminology. The use of inconsistent terminology contributes to the reluctance with which the subject-matter information security risk management is approached. [44] Briers [45] observes that "the field of risk management and its various subdisciplines is riddled with terminology that is often unfamiliar to the uninitiated."

The following definitions have been adopted by the researcher, and are central to the discussion which follows:

---

40 National Institute of Standards and Technology, Stoneburner, Goguen, and Feringa *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology* Special Publication 800-30 (October 2001) E-2 2.

41 ibid.

42 (n 15) 116-117.

43 ibid.

44 Badenhorst *A Formal Approach to the Optimisation of Information Technology Risk Management* (1994 thesis RAU) 30.

45 (n 20) 24.

(i) Risk: [46]

"Within the context of this discussion risk is synonymous with IT-related risks, and represents the net mission impact considering :

(i) The probability that a particular threat source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability, and

(ii) The resulting impact if this should occur.

IT-related risks arise from legal liability or mission loss due to –

(i) Unauthorised (malicious or accidental) disclosure, modification, or destruction of information;

(ii) Unintentional errors and omissions;

(iii) IT disruptions due to natural or man-made disaster; or

(iv) Failure to exercise due care and diligence in the implementation and operation of the IT system." [47]

Risk may therefor be viewed as:

"the potential for harm or loss, best expressed as the answer to those four questions:

(i) What could happen? / What is the threat?

(ii) How bad could it be? / What is the impact or consequence?

(iii) How often might it happen? / What is the frequency? and

(iv) How certain are the answers to the first three questions? /Degree of confidence." [48]

---

46 The following definitions may also be advanced to explain the concept of risk. Pritchard *Risk Management: Concepts and guidance* (2001) 9 defines risk as: "…cumulative effect of the probability of uncertain occurrence that may positively or negatively affect objectives..."; Smullen (n 23) 5 defines risk as: "(r)isk relates to situations in which the outcome is uncertain and the benefits or costs of the different possible outcomes are not identical."; and Greenstein and Vasarhelyi *Electronic Commerce: Security, Risk Management and Control* (2002) 214 define risk within e-commerce arena as: "…the possibility of loss of confidential data, or the destruction, generation, or use of data or programs that physically, mentally or financially harm another party, as well as the possibility of harm to hardware...".

47 (n 40) 4.

48 Tipton and Krause *Information Security Management Handbook* Vol 1 (2000) 251.

(ii) Risk Assessment: [49]

"The process of identifying the risk to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. It forms a part of Risk Management, and is synonymous with Risk Analysis."[50]

(iii) Risk management: [51]

"The total process of identifying, controlling, and mitigating information system-related risks. It includes risk assessment, cost-benefit analysis, and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on mission and constraints due to policy regulations, and laws."

"Risk management characterises the overall process. The first phase, risk assessment, includes identification of the asset at risk and their value, risks that threaten a loss of that value, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, mitigation, or transfer of risk. The second phase, risk mitigation includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures. Risk management is a continuous process."[52]

---

49 Wixley and Everingham (n 9) 80 define risk assessment as: "…the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risk should be managed..."; Tipton and Krause (n 48) 251 are of the opinion that this concept represents "…the assignment of value to assets, threat frequency, consequence and other elements of change. The reported results of risk analysis can be said to provide an assessment or measurement of risk."

50 It is important to observe that the NIST view risk assessment and risk analysis as being synonyms. Risk analysis is defined by the Australian and New Zealand Risk Management Standard 4360: 1999 Bowden, Lane and Martin (n 15) 13 as: "…a systematic process to determine how often events may occur and the magnitude of the likely consequences...". For purposes of uniformity the researcher will make use of the term risk assessment in this dissertation.

51 Pritchard *Risk Management: Concepts and guidance* (2001) xvi defines risk management as: "…method of managing that concentrates on identifying and controlling the areas or events that have a potential of causing unwanted changes… it is no more and no less than informed management…". Bowden, Lane and Martin (n 15) xv view risk management as: "… a process of continuous improvement directed towards the effective management of potential opportunities and adverse effects…Risk management is a systematic application of management policies, processes, and procedures to the task of identifying, analyzing, assessing, treating, and monitoring risk." Greenstein and Vasarhelyi *Electronic Commerce: Security, Risk Management and Control* (2002) 251 go even further to state that risk management "…is a methodology for: (i) assessing the potential of future events that can cause adverse affects; and (ii) implementing cost-efficient strategies that can deal with these risks…".

52 (n 48) 251-152.

(iv) Threat:[53]

> "The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." [54]

(v) Vulnerability:[55]

> "A flaw or weakness in the system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a breach of security or violation of the system's security policy." [56]

6.3.2.5 Regulating risk management - a South African perspective

Great emphasis is placed on risk management in the King II Report on Corporate Governance 2002. Section 2 of the report has been devoted to this subject matter. [57]

In the introduction to this section reference is made to the following remark by Levitt:[58] "The average company today is a complex enterprise engulfed by rapid technological change and fierce global competition. You have to assess exposure to risk on an ever changing landscape."

---

53 The President's Commission on Critical Infrastructure Protection (PCCIP), as established by President Clinton, is of the opinion that the term "threat" includes: "…anyone with the capability, technology, opportunity, and intent to do harm. Potential threats can be foreign or domestic, internal or external, state-sponsored or a single rogue element. Terrorists, insiders, disgruntled employees, and hackers are included in this profile...". The mandate of this commission is "…recommending a national strategy for protecting and assuring critical infrastructures from physical and cyber threats…" Greenstein and Vasarhelyi *Electronic Commerce: Security, Risk Management and Control* (2002) 214; Tipton and Krause (n 48) 555 define a threat as: "…the potential to cause harm to the corporation - intentional or otherwise...".

54 (n 48) 12.

55 Tipton and Krause (n 48) 555 define a vulnerability as: "…a weakness or threat to the asset..." they go on to observe "(t)he term characterises the absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both." Tipton and Krause (n 48) 152.

56 (n 48) 15.

57 (n 35) 73-85.

58 Arthur Levitt, Former chairperson of the U.S. Securities Exchange Commission. King II (n 35) 73.

From the outset the report acknowledges that risk is a fundamental part of doing business.[59] It is in fact the cost of doing business.[60] Risk management is seen as an inherent operational function and responsibility.[61] It is therefor contended by the report that the board committee, comprising of executive directors and senior management, will be in the best position to evaluate the risks facing the organisation and report on their findings.[62]

The report goes on to define risk as " …uncertain future events that could influence the achievement of a company's objectives",[63] and risk management is viewed as "the identification and evaluation of actual and potential risk areas as they pertain to the company as a total entity, followed by a process of either termination, transfer, acceptance (tolerance) or mitigation of each risk."[64]

The report ascribes accountability for risk management in no uncertain terms to designated role-players. What follows is a brief description of the responsibilities of each of these role-players.

Primary role-players:

6.3.2.5.1 Responsibilities of the board

The responsibility for risk management in its entirety is placed firmly in the hands of the board. [65] Although it cannot be expected of the board to be involved in the details of the development, implementation and administration of the risk management process, the board must gain assurance that risks are identified, evaluated, monitored, addressed and

---

59 (n 35) 73.
60 ibid.
61 ibid.
62 (n 35) 74.
63 (n 35) 73.
64 ibid.
65 (n 35) 75.

reported on, on an annual basis. [66] "Risk identification is ultimately the job of top management and the board of directors. But they must rely on people more directly engaged in the daily business for information." [67]

Furthermore the board is charged with the responsibility of reviewing the effectiveness of these processes, as well as setting in place and evaluating, strategies and policies dealing with risk management. [68]

The following falls within the scope of the board's responsibilities:

(i) The board is required to manage risks associated with information technology; [69]

(ii) The responsibility to decide which risks are deemed to be acceptable, and which are not in the pursuit of the company's mission, goals and objectives are placed within the board's scope of responsibility; [70] This would involve formulating a risk strategy, which would reflect the organisation's "appetite for risk"; [71]

(iii) The board is responsible for gaining assurance that a continuous process of risk assessment and management is in place, and that the results delivered by this process are acted upon in a timely fashion; [72]

(iv) The board will be responsible for instituting controls to mitigate and/or reduce the risks faced by the organisation, as well as for the formal review of these processes; [73]

(v) It is expected of directors to educate themselves on the risk management process employed by their company in order to gain a comprehensive understanding of the process; [74]

---

66 ibid.
67 (n 9) 80.
68 (n 35) 75.
69 (n 35) 77.
70 (n 35) 74.
71 (n 20) 17.
72 (n 35) 83.
73 ibid.
74 (n 35) 79.

(vi) The report acknowledges that risk management is a continuous process and places a duty on the board to ensure that the risk management process is thoroughly documented, reviewed and re-assessed on an annual basis;[75]

(vii) It is expected of the board to keep in mind changes that may occur in the internal, as well as the external business environment of the organisation.[76] The board must furthermore give careful consideration to the following:

(a) The question whether or not the company's objectives are being achieved, and if not what reasons may be advanced for this? [77]

(b) Are the objectives that were set for the risk management process being achieved?[78]

(c) Is the company flexible enough to respond quickly to changes in the external or internal environment? [79]

(d) Consider the quality as well as extent of management's monitoring and reporting duties;

(e) Are the communication channels of the organisation functioning effectively and keeping every employee informed about security-related issues?[80] and

(f) How effectively the company's reporting process is functioning? [81]

(viii) The board is furthermore placed under the obligation to disclose in the company's annual report the following information:

(a) The risk management process utilised by the company, as well as the person(s)/group responsible for the performance of this process; [82]

---

75 (n 35) 77.
76 (n 35) 82.
77 ibid.
78 ibid.
79 ibid.
80 ibid.
81 ibid.
82 (n 35) 77.

(b) Risk tolerance of the company; [83]

(c) The existence of an effective risk assessment program, which is monitored, evaluated and reviewed on a continuous basis. This would include a description of the process; [84]

(d) Assurance that a system of internal controls are in place to mitigate formidable risks faced by the organisation. [85] This would include a description of the internal controls utilised, as well as a description of the way in which these controls are reviewed; [86]

(e) Assurance that there is a disaster recovery plan[87] in existence that is documented and made known to all concerned. [88] This plan is to be used in case of a severe security incident in order to ensure that the company's critical business processes are not disrupted in such a manner that the company stops functioning altogether; [89]

(f) Additional information that may succour the reader in better understanding the risk management process of the company; [90] and

(g) A statement acknowledging that the ultimate responsibility for risk management and internal controls are vested in the board of directors. [91]

To assist the board in discharging the multitude of onerous responsibilities, the report allows for the appointment of a committee to review not only the risk management process, but also the risks facing the organisation. [92]

---

83 ibid.
84 (n 35) 84.
85 ibid.
86 ibid.
87 A disaster recovery plan has two major objectives: (i) "…timely recovery of mission critical business processes following a damaging event"; and (ii) "…the return to normal operations as soon as possible" Tipton and Krause (n 48) 583.
88 (n 35) 85.
89 ibid.
90 ibid.
91 (n 35) 84.
92 (n 35) 76.

6.3.2.5.2 Responsibilities of management

Management is accountable (answerable) to the board in respect of the following business concerns which falls within their domain of responsibility:

(i) The development, implementation, monitoring and evaluation of the risk management process; [93]and
(ii) Making the process of risk management and internal controls a part of the organisation's daily routine. [94]

It is the responsibility of management to report to the board on significant risks facing the organisation, as well as on the effectiveness of internal controls implemented for the purpose of reducing and mitigating these risks. [95]

Secondary role-players

6.3.2.5.3 Responsibilities of the dedicated committee

This committee[96] will be responsible for investigating and reporting on how effectively the risk management process is functioning on operational level. [97] It will also be responsible for monitoring the risk strategy and policy as well as reporting on its findings. [98] It is recommended that a member of the board should chair the committee. [99] The committee will:

(i) "Monitor the risk management's performance by looking for assurance that the program is linking risk to value;

---

93 (n 35) 75.
94 ibid.
95 ibid.
96 It is recommended that this committee be called the "Executive Risk Management Committee" Briers (n 20) 17.
97 (n 35) 76.
98 ibid.
99 (n 20) 17.

(ii) Monitor the program's standards and make sure that its code of practice and policies are current according to best practice;

(iii) Monitor the resources being allocated to the various risk functions;

(iv) Monitor cost associated with risk protection; and

(v) Monitor the development of a risk culture within the organisation."[100]

6.3.2.5.4 Responsibility of the company as a whole

Risk management, as well as internal controls must form an integral part of the daily activities of the company, thereby becoming a habitual action of all employees. This will foster a culture of security within the organisation.[101]

The report recommends that the company develops a system of risk management and internal controls that embodies the following outcomes:

(i) Displays the existence of a dynamic risk identification program;[102]

(ii) Illustrates management's commitment to the processes;[103]

(iii) Demonstrates the risk mitigation process employed by the company; [104]

(iv) Document all risk-related communication, the cost of non-compliance, and the system of risk management and internal controls utilised by the company; [105] and

---

100 (n 20) 18-19.
101 (n 35) 75.
102 (n 35) 81.
103 ibid.
104 ibid.
105 ibid.

(v) Construct a database of formidable risks faced by the organisation.[106]

6.3.2.6 Problems associated with information security risk management

A prevalent problem that is encountered when dealing with risk management is that the following facets of risk management are not properly understood:

(i) Which risk, threats and vulnerabilities exist;[107]

(ii) Which assets of the organisation should be protected;[108]

(iii) Which countermeasures and controls are available;[109] and

(iv) How to calculate the damage that may ensue.[110]

It may furthermore be observed that top management has no problem accepting that financial risk management forms an integral part of every organisation, yet the issue of technology-related risk management is still approached with skepticism and apprehension by some. Badenhorst[111] advances the following reasons that might explain why risk management in the technology arena finds itself in such a predicament:

(i) The concept of "risk" is not fully understood, as it is seen as a very subjective concept that involves a lot of guesswork.[112] This discipline is not based on hard concrete facts or scientific calculations which are logical, meticulous and precise;

(ii) Risk related terminology used in most literature are very confusing, as it appears that the concepts of risk analysis, risk assessment and risk management are used intercurrently without

---

106 ibid.
107 Mizuno "Risk management of corporations on the Internet" (last visited 15 August 2002) http://ifrm.glocom.ac.jp/gii/mizuno 19990831en.html 1.
108 ibid.
109 ibid.
110 ibid.
111 (n 44) 9-10.
112 (n 44) 9.

proper regard being given to their true meaning and interpretation;[113]

(iii) Information technology department management often view risk management as a luxury. [114] They rather prefer to be spending their already tight budget on much more profitable areas that can be seen to deliver tangible benefits and results. This problem is exacerbated by the fact that the value of information security is often very difficult to quantify, as it delivers almost no tangible benefits, but rather acts as a preventative exercise;[115]

(iv) It is generally assumed and taken for granted that information security personnel will possess over the necessary knowledge and skills concerning risk management and risk assessment. [116] This in turn results in these processes mostly focussing on the technological aspects thereof, often ignoring the business side of risk management altogether; [117]

(v) Information security departments are in general hesitant to disclose how vulnerable the information assets of the organisation are. [118] They would rather assume the appearance that their information security is unbreakable, than acknowledge the reality that a hundred percent secure environment represent an unattainable dream. Furthermore, the information security department is very reluctant to outsource its risk management function, as they feel such valuable information could be fatal in the hands of their competitors. [119] Not only can outsourcing open the door for industrial espionage, but such an objective view from a neutral third party might reflect negatively on the department itself,

---

113 ibid.
114 ibid.
115 (n 48) 589.
116 (n 40) 9.
117 ibid.
118 ibid.
119 ibid.

resulting in the perception that the department is ineffective, unproductive or not capable of holding its own; [120]

(vi) Not only are information security departments within the organisation concealing security incidents, but if such incidents are eventually disclosed to management, they themselves will do their best to try and hide security breaches for fear of public embarrassment, damage to reputation and a loss of shareholder confidence.[121] Consequently:

> "…no credible statistics concerning the total amount of financial loss resulting from security-related intrusion are available, but judging from the amount of money corporations and government agencies are spending to implement Internet and other security controls, the cost must be extremely high."[122]

(vii) Another problem facing organisations is the complexity and inflexibility associated with available risk management models; [123]

(viii) Risk management models available to organisations require a high level of resource investment, such as time, money and skilled personnel, none of which organisations have an abundance of in the present economic climate; [124]

(ix) Technology changes and developments occur on a seemingly daily basis at the speed of light. The rate at which present technology is becoming obsolete petrifies even the most fierce information security manager.[125] It is a well-known fact that new technology will inevitably be followed by new and even greater risks, threats and vulnerabilities; [126] and

---

120 ibid.
121 (n 48) 73.
122 ibid.
123 (n 40) 9.
124 (n 40) 10.
125 (n 48) 287.
126 ibid.

(x) A recent paper issued by Ernst & Young[127] identified the following factors as being the main culprits responsible for the growing risk in security breaches:

(a) Under-funding;[128]

(b) Recruitment shortage;[129] and

(c) Poor procedural practice.[130]

Ernst & Young[131] went even further to identify under-funding (under-spending) as the worst problem. This problem may be attributed to the fact that it is very difficult to estimate and/or calculate a precise monetary value of a potential risk.[132] Even if the risk materialises, calculating the cost of damage that has occurred can be an all but impossible task. How do you calculate the damage to an organisation's good name or reputation, or the loss of customer confidence? Ernst & Young[133] therefor recommends that organisations ask themselves the following questions:

(a) Over what information assets do the organisation possess? (Inventory)[134]

(b) What needs to be protected?[135]

(c) Is the information worth protecting?[136]

(d) What are the key vulnerabilities?[137] and

(e) Is connectivity the organisation's key vulnerability?[138]

---

127 Ernst & Young "Risk to information security identified" (last visited 20 August 2002) http://www.itweb.co.za 1-2.
128 (n 127) 1.
129 ibid.
130 ibid.
131 ibid.
132 ibid.
133 (n 127) 1-2.
134 (n 127) 2.
135 ibid.
136 ibid.
137 ibid.
138 ibid.

It should be evident from the preceding discussion that there are numerous challenges facing organisations who wish to implement information security risk management into their organisation. It is however essential that directors and top management overcome these hurdles and seek solutions for these problems, as an inadequate risk management practice may expose the organisation to:

(i) Civil claims; [139]
(ii) Cost of sanctions (fines, imprisonment, personal liability of directors and managers); [140]
(iii) Adverse publicity; [141]
(iv) Loss of staff morale; [142]
(v) Legal cost in defending criminal and civil actions; [143] and
(vi) Revocation of regulatory licenses and permits. [144]

6.3.2.7 Risk management - the process

6.3.2.7.1 Introduction

Information Security has as its objective the following outcomes:[145]

(i) Maintain customer, constituent, stockholder, and taxpayer confidence in the organisation;
(ii) Protect confidentiality of sensitive information;
(iii) Protect sensitive operational data from inappropriate disclosure;
(iv) Avoid third-party liability resulting from illegal or malicious acts committed with the organisation's systems;

---

139 (n 15) 5.
140 ibid.
141 ibid.
142 ibid.
143 ibid.
144 (n 15) 6.
145 (n 8) 16.

(v) Ensure that the organisation's computers, network, and data are not misused or wasted;

(vi) Avoid fraud;

(vii) Avoid expensive and disruptive incidents;

(viii) Comply with pertinent laws and regulations;[146] and

(ix) Avoid a hostile workplace atmosphere.

These information security objectives are supported by five risk management principles, which in turn constitute the risk management life cycle.

[146] See Annexure A for a comprehensive list of information security legislation, regulations, and standards.

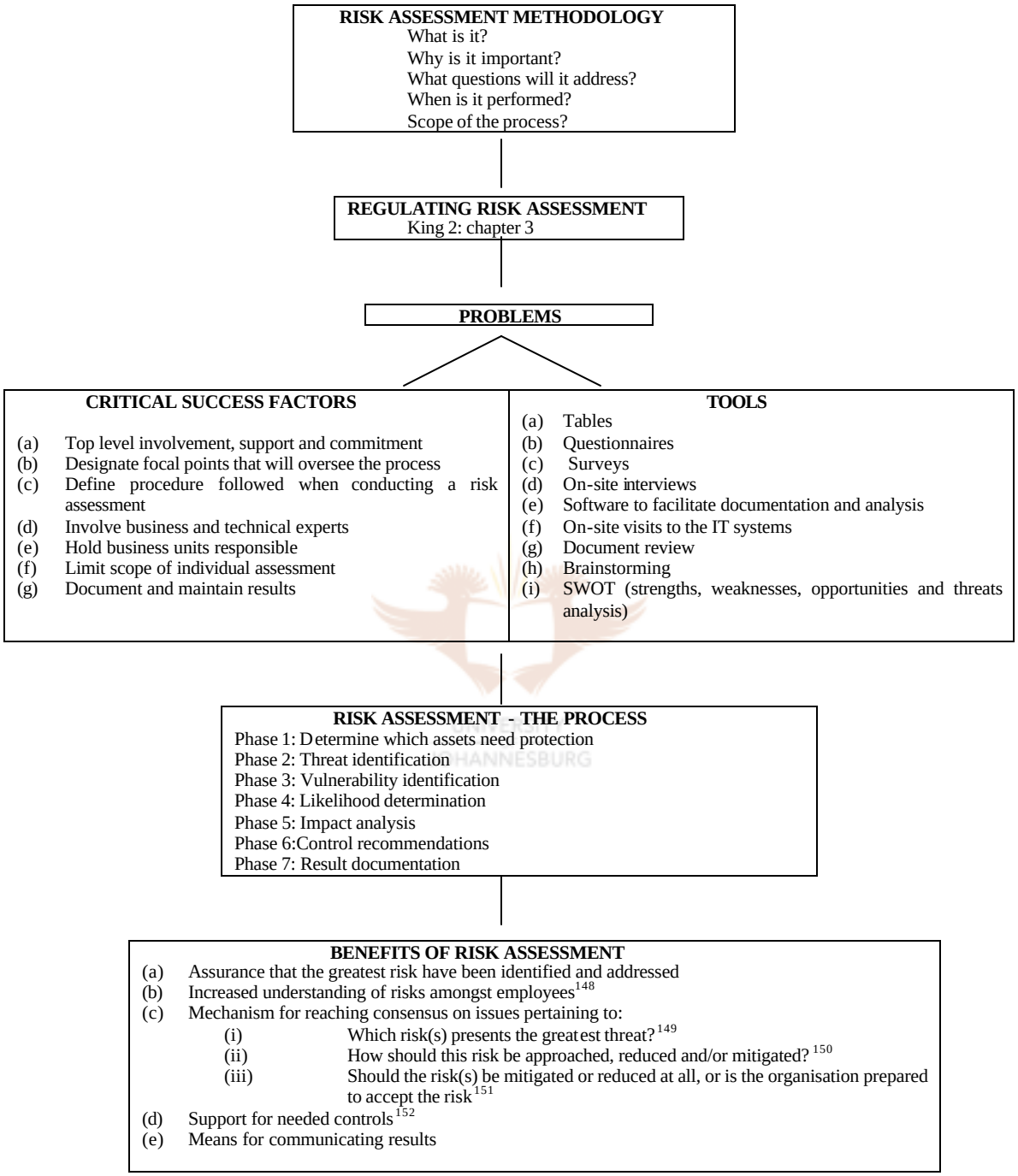
6.3.2.7.2 Framework for the implementation of the risk management life cycle[147]

Principle	Practice
1. Assess risk and determine needs	1. Recognise information resources as essential organisational assets. 2. Develop practical risk assessment procedures that link security to business needs. 3. Hold program and business managers accountable. 4. Manage risk on a continuous basis.
2. Establish a central management focal point	5. Designate a central group to carry out key activities. 6. Provide the central group ready and independent access to senior executives. 7. Designate dedicated funding and staffing. 8. Enhance staff professionalism and technical skills.
3. Implement appropriate policies and related controls	9. Link policies to business risks. 10. Distinguish between policies and guidelines. 11. Support policies through the central security group.
4. Promote awareness	12. Continually educate users and others on risks and related policies. 13. Use attention-getting and user-friendly techniques.
5. Monitor and evaluate policy and control effectiveness	14. Monitor factors that affect risk and indicate security effectiveness. 15. Use results to direct future efforts and hold managers accountable. 16. Be alert to new monitoring tools and techniques.

As stated earlier, risk management comprises of two principal components/phases, namely: (i) risk assessment; and (ii) risk mitigation.

[147] (n 8) 20.

6.3.2.8 PHASE 1: RISK ASSESSMENT ROADMAP TO RISK ASSESSMENT



[148] (n 15) 234.

[149] United States General Accounting Office Accounting and Information Management Division *Information Security Risk Assessment: Practices of Leading Organisations* GAO/AIMD-99-139 (August 1999) 18.

[150] ibid.

[151] ibid.

[152] Hunter *Information Security: Raising Awareness* (May 2000) 33.

6.3.2.8.1 Risk assessment methodology

(i) Defining risk assessment

> "Risk assessment, whether they pertain to information security or any other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes, and make informed judgements concerning the extent of actions needed to reduce risk."[153]

Risk assessment is concerned with ascertaining the extent of a potential threat, and evaluating the results in order to decide on appropriate controls and countermeasures to be implemented to reduce or mitigate the risk based on the likelihood of the threat materialising and the estimated impact of such an event. [154] The goal of risk assessment is to reduce the risk to an acceptable level.

Risk assessment is the first step in the risk management life cycle, and may be viewed as one of the essential elements of the risk management concept. [155]

(ii) Need for risk assessment

The question may be asked why risk assessment should be performed in the first place. The answer to this question lies in the fact that it is required of directors and top management to discharge their responsibility of due diligence in the decision-making process.[156] By having documented proof that risk assessment has been performed they will be one step closer to discharging this onerous responsibility.[157] A second reason that may be advanced to support the need for risk assessment is that it eliminates redundant, outdated controls and measures that might in fact be inhibiting performance. Risk

---

153 (n 149) 7.
154 (n 152) 33.
155 ibid.
156 (n 11) 1.
157 (n 35) 77.

assessment will ensure that the most effective risk measures and controls are implemented.

(iii) Questions a risk assessment process will address

(a) What risks face the organisation?[158]

(b) How likely is this risk to materialise? [159] and

(c) If the risk does materialise what effect/impact will it have on the organisation? [160]

(iv) Performance of risk assessment

According to research done by the GAO[161] most risk assessments are performed under the following circumstances:

(a) After a serious security incident have occurred; [162]

(b) Whenever a new risk/vulnerability is discovered; [163] or

(c) Whenever a new project, task, development cycle, system or application is started.[164]

It is recommended by the King II report[165] that the performance of a risk assessment should at least be considered when:

(a) Significant changes occur in the operating environment;[166]

(b) When new personnel, new products and activities, or new and

---

158 (n 20) 13.
159 ibid.
160 ibid.
161 Hamilton "New trends in risk assessment" *Data Security Management AIMS* (April 1995) 21.
162 ibid.
163 ibid.
164 (n 11) 1.
165 (n 35) 78.
166 ibid.

improved information systems are introduced into the organisation;[167] and

(c) In case of corporate restructuring, acquisitions and disposals, or changes in foreign operations. [168]

It is contended by Peltier[169] that a risk assessment process should take only a few days. Weeks or months are out of the question. Organisations who have implemented an effective risk assessment process should be flexible enough to execute this process using the minimum resources, yet still delivering the maximum results in the form a complete, accurate and timely information on risks facing the organisation. Organisations should not be discouraged by the fact that the initial risk assessment process will be time and resource consuming. As the process becomes more refined and is used more often, it will go quicker. Furthermore, ensure that all relevant role players are involved in this process, from top management right down to internal experts.[170]

(v) The scope of the risk assessment process

It is contended by the King II report[171] that risk assessment should at minimum focus on the company's exposure to:

(a) Physical and operational risks; [172]

(b) Human resources risks; [173]

(c) Technology risks;[174]

(d) Business continuity and disaster recovery; [175]

---

167 ibid.
168 ibid.
169 (n 11) 2.
170 Internal experts may be viewed as those people responsible for the development and implementation of a system.
171 (n 35) 77.
172 ibid.
173 ibid.
174 ibid.
175 ibid.

(e) Credit and market risks; [176] and

(f) Compliance risks. [177]

6.3.2.8.2 Regulating risk assessment : Risk assessment in the light of the King II report

The King II report addresses the concept of risk assessment in chapter three.[178] The report characterises risk assessment as a continuous process of identifying the most significant risks and/or threats facing the organisation. [179] It goes on to recommend that risk assessment should be undertaken on an annual basis with regular reviews of the results delivered by the process**.**[180] Management will be responsible for the development and implementation of the risk assessment program.[181]

6.3.2.8.3 Problems associated with information security risk assessment

It is contended by the researcher that the task of information security risk assessment is much more daunting and challenging than those associated with other types of risks. Some reasons that may be advanced to support this statement are the following:

(i) Information on risk factors are limited, [182] for example the likelihood of a hacker attacking and the cost of damages or losses as a result of exploitation of security weakness are all very subjective, imprecise and vague factors; [183]

---

176 ibid.
177 ibid.
178 (n 35) 78.
179 ibid.
180 ibid.
181 (n 20) 17.
182 (n 149) 8.
183 ibid.

(ii) Risk factors are ever changing and these changes are occurring at a staggering pace; [184]

(iii) Loss and damages that may result because of information security breaches are very hard to quantify, for instance loss of customer confidence or loss of reputation, may result in immeasurable and irreparable damage to an organisation's image and reputation; [185]

(iv) There is a negative side to the rapid rate at which technology is developing – intruders are becoming more sophisticated, and the tools that they use are becoming more readily available.[186] Unlike most organisations, intruders (hackers and crackers) are growing with technology, and are not disheartened or deterred by it. They are using it to their full advantage; [187]

(v) In most organisations some degree of resistance to risk assessment will be encountered. The reluctance with which risk assessment is approached may be ascribed to:

(a) Ignorance of management regarding risk assessment; [188]

(b) Arrogance – management still do not realise that information security will contribute to the bottom line;[189] and

(c) Fear – managers are petrified of acknowledging that they do not operate in a secure environment. Fear of realising that there are risks, vulnerabilities and threats existing within the organisation that needs to be addressed, but are not. [190]

(vi) Organisations still tend to make use of outdated information. Up-to-date, current data is needed otherwise the risk assessment

---

184 (n 149) 9.
185 ibid.
186 Tipton and Krause *Information Security Management Handbook* Vol 2 (2001) 453.
187 ibid.
188 (n 48) 258.
189 ibid.
190 ibid.

process will result in an ineffective fruitless exercise that will be a waist of valuable resources;

(vii) Risk assessment, especially in its initial stages, are very time consuming, and this may proof to be discouraging for top management and employees alike who want to witness immediate results; [191]

(viii) It has been argued that traditional risk assessments do not distinguish between security and privacy concerns.[192] What the organisation views as a security concern, the customer or client regard as a privacy concern; [193] and

(ix) The quantification of risk is an extremely difficult notion, yet:

> "risk quantification is at the core of all activities for traders, corporate treasurers and market makers. They worry about how much money they stand to make or loose given their current position."[194]

The following reasons may be advanced why the subject of risk quantification is approached with such apprehension:

(i) Many "attacks" within the organisation are never reported because:

(a) attacks / vulnerabilities / intruders are never discovered,[195] and/or

(b) business managers are reluctant to disclose to top-level management that their department or unit have been the victim of an attack, for fear of this reflecting badly on their work

191 (n 48) 259.
192 (n 152) 30.
193 ibid.
194 Alexander (ed) *Risk Management and Analysis: Volume 1: Measuring and Modeling Financial Risk* (1998) 48.
195 (n 8) 25.

performance, or worse still, for fear of losing their jobs. [196]

(ii) Limited data exist relating to the cost associated with certain security weaknesses. [197]

The convergence of all these factors make it very difficult, if not impossible to indicate how the cost associated with control measures will limit or reduce the risk. [198] It is ultimately expected of business managers to make the best possible use of available information by, for instance visiting web sites, keeping up-to-date with available literature on computer security risks, vulnerabilities and threats, reading bulletins on the subject-matter and attending seminars. [199] They should also rely on the judgement of knowledgeable individuals to ensure that cost-effective countermeasures are in place.[200]

6.3.2.8.4 Critical success factors

Seven critical success factors to the risk assessment process may be identified:

(i) Top level involvement, support and commitment;[201]

(ii) Designate focal points that will oversee the process; [202]

(iii) Define procedure to be followed when conducting a risk assessment;[203]

(iv) Involve business and technical experts; [204]

(v) Hold business units responsible; [205]

(vi) Limit scope of individual assessment; [206] and

---

196 ibid.
197 ibid.
198 ibid.
199 (n 8) 26.
200 ibid.
201 (n 149) 11.
202 ibid.
203 ibid.
204 ibid.
205 ibid.
206 ibid.

(vii) Document and maintain results. [207]

6.3.2.8.5 Risk assessment tools[208]

The following tools might aid organisations when performing a risk assessment:

(i) Tables;

(ii) Questionnaires;[209]

(iii) Standard report formats;

(iv) Surveys;[210]

(v) On-site interviews;[211]

(vi) Software to facilitate documentation and analysis;

(vii) List of threats and controls;

(viii) On-site visits to the IT systems;

---

[207] ibid.

[208] These tools may be used in conjunction with one another.

[209] The following guidelines should be kept in mind when drafting questions to be used in questionnaires:

(i) The questions advanced to an employee should be directly linked to a control standard or objective;

(ii) The number of questions asked to an employee must be limited;

(iii) Employees need to be reassured that the questions are just a method of information gathering, and does not in any way cast doubt on their work performance;

(iv) It is recommended that questions are divided into functional areas, this eliminates the possibility that an employee will waste valuable time answering questions regarding issues that do not fall within his job category or description; and

(v) It is highly recommended that questionnaires make provision for the employees to make recommendations, voice concerns or simply make comments. Hamilton "New trends in risk assessment, data security management" *AIMS* (April 1995) 9.

See Annexure H for an example of a standardised risk assessment questionnaire.

[210] McLeod and Schell *Management Information Systems* (2001) 129.

[211] It is contended by McLeod Jr. and Schell (n 210) 129 that personal interviews are the preferred method of information gathering as numerious benefits are derived from this method, including:

(i) "It provides the opportunity for two-way communication and observation of body language;

(ii) It can stimulate enthusiasm for the project on the part of both the information specialist and the users;

(iii) It can establish a common bond of trust between the users and the information specialists; and

(iv) It provides the opportunity for the participants in the project to express different, even opposing views."

See Annexure I for sample interview questions.

(ix) Document review;[212]

(x) Brainstorming;[213] and

(xi) SWOT (strengths, weaknesses, opportunities and threats) analysis.[214]

[212] Policy documentation (legislation and directives); security documentation (previous risk assessment reports, audit reports and security policies); system documentation (systems user guide and manual)" should be studied NIST (n 40) 12. For more information on the actual process of documentation reviews, consult Pritchard *Risk Management: Concepts and guidance* (2001) 83-89.

[213] Pritchard *Risk Management: Concepts and guidance* (2001) 309 defines brainstorming as: "…a problem solving technique that can be used for planning purposes, risk identification, improvement efforts and other project-related endeavors…".

[214] For a discussion on SWOT, consult Pritchard (n 213) 129-135.

6.3.2.8.6 Risk assessment – the process [215]

Goal	Step	Result Delivered
Defines scope of risk assessment process	**Step 1: System characterisation**	Inventory of what the information security environment comprises of, in order to determine which information assets needs protection.
Identify possible threat-sources	**Step 2: Threat identification**	Draft a threat statement identifying threat sources and their motivation.
List potential vulnerabilities that can be exploited by threat-sources	**Step 3: Vulnerability identification**	Delivers a condensed list of system vulnerabilities.
Determine the likelihood that a vulnerability will be exploited	**Step 4: Likelihood determination**	Ranking of the likelihood that a vulnerability will be exploited (high, medium or low).
Determine what would be the result if a threat successfully exploits a vulnerability	**Step 5: Impact analysis**	Calculation of the estimated impact (high, medium or low).
Identify controls that would effectively reduce and/or minimise or eliminate those risks previously identified	**Step 6: Control recommendations**	Identify controls that may be utilised effectively.
Compile a risk assessment report that will give an overview of threats and vulnerabilities identified, measurement of the risk, and recommended controls	**Step 7: Result documentation**	Drafting of a risk assessment report.

The researcher does not attempt to make directors or top management experts in any of the components of risk, but merely to provide them with a foundation for the development and implementation of an effective risk management process.

[215] The framework used by the researcher is based on the diagram developed by the National Institute of Standards and Technology (henceforth NIST). This framework has been adapted and modified by the researcher so that the importance thereof within an information security governance setting may be captured and conveyed. NIST (n 40) 8.

Consequently, the researcher only discusses those steps that will be of significant value for purposes of this dissertation.

Phase 1: Determine which assets need protection

Goal: Determine which information assets exist within the organisation, and the level of protection they require.

It is necessary to determine which assets are important and valuable to the organisation in order to ultimately determine which assets warrant protection. [216] To uncover the essence and value of an asset it is recommended that the following questions be considered:

(i) "What are you trying to protect?

(ii) How much is it worth? and

(iii) How much depend on it?" [217]

Assets may be physical, logical, tangible or intangible in nature. The only prerequisite is that the asset should hold some kind of value for the organisation. [218] When determining the value an information asset holds for the oganisation it is recommended that attention is focused on:

(i) What is the cost associated with the production, as well a reproduction of the information, if it were to be damaged, lost, altered, released or destroyed? [219]

(ii) What consequences would ensue if information were unavailable to the organisation? [220]

(iii) Would a breach in information security result in any one of the following: loss of customer confidence, damage to the organisation's reputation, or loss of its competitive advantage? [221]

---

[216] (n 40) 11.
[217] ibid.
[218] ibid.
[219] (n 11) 5.
[220] ibid.
[221] ibid.

(iv) What is the value of the information on the open market and to the organisation's competitors? [222] and

(v) Which benefits are associated with the information held by the organisation? [223]

The process of information classification must be performed by business and unit managers, therefor those people who use the information on a regular basis.[224] The pivotal importance of information classification is reflected in Napoleon's[225] maxim "he who defends everything, defends nothing!". Consequently, "if the organisation does not stratify or prioritize its information assets it is likely to spend too much time and money protecting the 'crown jewels' and mundane, low-value information equally."[226]

Four categories of asset classification exist:

Critical applications or data	**Confidential information**	**Sensitive information**[227]	**Public information**
This type of data or information is of such crucial importance for the continued existence of the organisation that its loss or damage will proof to be pernicious to the organisation. [228]	This type of information or data must specifically be protected against unauthorised disclosure, access and distribution. [229]	This type of data or information must be protected against alteration, modification or destruction. [230] The most important factor when dealing with sensitive information is ensuring that its integrity remains in tact.	This type of information is not regarded as confidential, but might still be seen as sensitive.[231]

222 ibid.
223 ibid.
224 Business managers generally distinguish between confidential information and proprietary information based on "…the competitive advantage that accrues to the organisation by managing dissemination of the information…" Tipton and Krause (n 48) 293.
225 (n 48) 293.
226 ibid.
227 Examples of sensitive information may include the organisation's financial and legal statements, records and documents.
228 Martinez *Integrated Risk Management – A Concept for Risk Containment* (2001) 7-8.
229 ibid.
230 ibid.
231 ibid.

Security has as its first and foremost objective the protection of integrity, availability and confidentiality of information or data.[232] It is therefor recommended that the impact of a security breach must be described in terms of the effect of loss or degradation on any one of these attributes.[233]

(i) **Loss of integrity:** Entails the protection of information against unauthorised modification.[234] This can occur accidentally or intentionally, and will result in decisions being based on unreliable, erroneous information.[235]

(ii) **Loss of availability:** Entails that critical information assets are unavailable to users. This will result in loss of efficiency with which services are delivered and products are produced.[236]

(iii) **Loss of confidentiality:** Refers to the protection of data/information against unauthorised disclosure.[237] This may result in loss of customer/client confidence, and/or damage to reputation of the organisation.[238]

Result delivered by phase 1: a comprehensive overall picture of those information assets the organisation needs to protect.

---

232 (n 8) 22.
233 For a comprehensive discussion of these three pillars/attributes, as well as an additional three, refer to chapter 2.
234 (n 186) 130.
235 (n 8) 22.
236 ibid.
237 (n 48) 406.
238 (n 8) 22.

Phase 2: Threat identification - understanding the risk [239]

"[Threat identification] is an important exercise to undertake since the identification of risk is one of the first major steps in managing risk."[240]

Goal: identify potential threat-sources to the organisation that can adversely impact on valuable assets, and compile a threat statement listing potential threat-sources. [241]

It should be kept in mind that risk management does not start with the risk. Risk will only become a consideration once it is threatening to negatively affect the goals, mission, objectives or assets of the organisation. [242]

To fully comprehend the potential threats facing an organisation the following components must be understood:

1) **Threat Agent/ Source** (Adversary) – Threat agents may be seen as those elements responsible for initiating attacks against computers.[243] The threat may originate from an internal or external source.[244]

   Threat agents may be subdivided into three main categories:

   (i) Human; [245]

   (ii) Nature; [246] and

   (iii) Environmental. [247]

---

239 As observed by Bowden, Lane and Martin (n 15) 50, threat identification and characterisation is a very subjective exercise that will be influenced by each individual employee's believes, training and experience.

240 (n 23) 87.

241 (n 15) 50.

242 Duffield "E-business risk management" (last visited 18 April 2002) http://www.itweb.co.za 2.

243 (n 152) 5.

244 (n 186) 570.

245 (n 40) 13.

246 ibid.

247 ibid.

2) **Motive** (Objective) – The motive represents the driving force behind the threat-agent's actions.[248] It may be subdivided into two main categories:

(i) Intentional; [249] or
(ii) Accidental. [250]

3) **Result/Impact** – The result depicts what the consequence of the act "performed" by the agent would be. Examples of this may include:

(i) Consumer/business partner's confidence lost;
(ii) Critical operations halted;
(iii) Sensitive data disclosed;
(iv) Services and benefits disrupted;
(v) Asset loss;
(vi) Damage to the reputation of organisation;
(vii) System downtime;
(viii) Loss of information;
(ix) Loss of access;
(x) Destruction of information; and
(xi) Unauthorised disclosure of information.

[248] ibid.
[249] (n 40) 12.
[250] ibid.

(i) Identification of the threat-source/agent (Adversaries)[251]

A threat agent/source possess over the capacity to inflict damage and harm directly to the IT system, and indirectly to the organisation. [252]

[251] Schneier *Secrets and Lies* (2000) 42 observes that the type of threat-agents menacing organisations are still the same as those found in the physical world: "(c)ommon criminals looking for financial gain, industrial spies looking for a competitive advantage, hackers looking for secret knowledge, military intelligence agencies looking for military intelligence. People haven't changed it is just that cyberspace is a new place to ply their trades…" NIST (n 40) 13.

[252] The diagram which follows is based on a framework developed by NIST (n 40) 13.

Threat-source[253]	**Examples**
Natural threat[254]	Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, cyclones, hail, monsoon, sandstorms, tsunami, snow, hurricanes.[255]
Human threat	Human threats may be subdivided into: **1. Unintentional acts** This act was not performed on purpose. It lacks the necessary motivation and/or intention to cause harm. Examples of unintentional acts include: errors, accidents or negligence. **2. Intentional acts** These are deliberate attacks performed by for instance, malicious person's or disgruntled employees gaining unauthorised access to information or disclosing classified information. Two of the most commonly found forms of deliberate/intentional attacks are: (a) Malignant attempts at unauthorised access to for instance, IT system in order to modify, alter, amend, damage or delete the integrity, availability and/or confidentiality of information/data; and (b) An altruistic endeavor to outwit system security.
Environmental threat	Long–term power failure, chemicals, pollution, and liquid leakage.

[253] The list of threats that follow should not be seen as an exhaustive list of threat-agents/sources. New threats and vulnerabilities are being discovered on a seemingly daily basis.

[254] For a more comprehensive list of natural threats the organisation might be confronted with search local and national weather sites.

[255] Greenstein and Vasarhelyi *Electronic Commerce: Security, Risk Management and Control* (2002) 259.

(ii) Motivation behind the threat (Objective)

Key to the success of any risk assessment process is to build consensus around the nature and motivation behind each of the threats identified, whether they are intentional or accidental. [256] In order to understand the motivation behind threat actions it will be useful to re-visit and recapitulate the following:

(a) History of system break-ins; [257]
(b) The security violation reports; [258] and
(c) The incident reports. [259]

When the motivation behind a threat is understood, it will be easier to decide on preventative measures to be employed.[260]

Intentional threats	**Accidental threats**
These threats are executed with a specific malevolent purpose or objective in mind.	These threats are usually not accompanied by an illegal motive, but materialise because of an accident. Therefor, no criminal connotation can be made to these threat-agents.

[256] Profile of a threat-agent:
(a) "The naïve: these attackers have little knowledge or experience. They are out to do it for fun, with no understanding of the potential consequences;
(b) Brutish (script kiddies): these attackers also lack real knowledge, and make heavy use of the various attack tools that exist. This means that they become obvious and visible on attacked systems due to the heavy probing and scanning used;
(c) Clueful: these are more experienced attackers, who use a variety of techniques to gain access to the system. These attacks are generally more subtle and less obvious; and
(d) Truly subtle: these are the computer criminals of the twenty-first century. They know what they want, who will pay for it, how to get access, and how to move around the system once they entered it. These attackers leave few or no traces on a system that they were in fact there" Tipton and Krause (n 186) 550.

[257] (n 8) 12.
[258] ibid.
[259] ibid.
[260] (n 11) 59.

(a) Alteration of data (b) Alteration of software (c) Bomb threat (d) Disclosure of information (e) Sabotage (f) Vandalism (g) Theft (h) Unauthorised use (i) Fraud	(a) Accidental disclosure of information (b) Electric disturbance (c) Electric interruption (d) Emanation (e) Liquid leakage (f) Human error made by users (g) Telecom interruption (h) Fire (i) Software error (j) Hardware failure

Interplay between the threat-agent, threat action, and motivation behind the threat:[261]

Threat-agent	Motivation	Threat action
Hacker and crackers[262]	Challenge Ego Rebellion	(a) Hacking[263] (b) Social-engineering[264] (c) System intrusion, break-ins (d) Unauthorised system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorised data alteration	(a) Computer crime (eg. staking) (b) Fraudulent acts (eg. impersonation, interception) (c) Information bribery (d) Spoofing (e) System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	(a) Bomb/Terrorism (b) Information warfare (c) System attack (d) System penetration (e) System tampering

[261] (n 40) 14.

[262] Tipton and Krause (n 186) 453 observe that traditionally hackers were defined as "…an individual who is focused on determining how things work and devising innovative approaches to addressing computer problems..." In contrast to these "noble" individuals we encounter crackers who are "…malicious attackers, who want to cause damage and mayhem…".

[263] For a comprehensive discussion on hacker tools and techniques, consult Tipton and Krause (n 186) 453-474.

[264] Tipton and Krause (n 48) 75 view social engineering as: "…fabricating a story to trick users, system administrators, or help desk personnel into providing information required to access systems. Intruders usually solicit passwords for user accounts, but information about the network infrastructure and the identity of individual hosts can also be the target of social engineering attacks…".

Industrial Espionage (Companies, or foreign governments, or other government interests)[265]	Competitive advantage Economic espionage	(a) Economic exploitation (b) Information theft (c) Intrusion on personal privacy (d) Social engineering (e) System penetration (f) Unauthorised system access
Insiders (Poorly trained, or disgruntled, or malicious, or negligent, or dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors	(a) Assault on an employee (b) Blackmail (c) Browsing of proprietary information (d) Computer abuse (e) Embezzlement (f) Fraud and theft (g) Information bribery[266] (h) Input of falsified, corrupted data (i) Malicious code (j) Sale of personal information (k) System bugs (l) System intrusion[267] (m) System sabotage (n) Unauthorised system access

(iii) The following factors could impact on the threat faced by the organisation

(a) Geographical location of the organisation; [268]

---

[265] Tipton and Krause (n 186) 552 define industrial spies as attackers who "…specifically target a particular company as a place from which to obtain information that they have been hired to collect, or that they believe will be considered valuable to others who will buy it...". The main objective of an industrial spy is to gain a competitive advantage by stealing trade secrets. A distinction should be drawn between industrial espionage and economic espionage. The former involves one organisation contracting another to perform the espionage on its behalf, the latter involves "…data collection that is authorised and driven by governments...".

[266] An attack can originate from inside or outside the organisation. There exist conflicting viewpoints regarding the question whether external or internal threats pose the greatest danger to organisations. There are those that feel that the biggest threats facing organisations originate from external sources. This comes as a direct result of the increased use of the Internet. Greenstein and Vasarhelyi (n 255) 215; and then there are those that believe the internal threat is still the greatest threat. Insiders have "…virtual unrestricted access to anything…" because of the fact that they have an authorised presence on the network. Tipton and Krause (n 186) 148, 551.

[267] Tipton and Krause (n 186) 572 define an intrusion attempt as "(t)he potential possibility of a deliberate unauthorised attempt to:

(i) access information;
(ii) manipulate information; and
(iii) render a system unreliable or unusable…".

[268] (n 11) 14.

(b) The facility the organisation is housed in;[269]

(c) The location surrounding, or near to the organisation; [270] and

(d) Who the organisation shares the facility with, thus its neighbours.[271]

(iv) Threat occurrence rate

Once the (i) valuable assets have been identified, and (ii) the threats facing these assets have been identified, it is necessary to establish a nexus between these two variables. A popular method utilised for this purpose is Annual Loss Expectancy (ALE).[272] This method uses the following formula:[273]

Single loss Expectancy	x	Annualized rate of Occurrence	=	Annualized loss Expectancy

In order to calculate the ALE the single loss expectancy (SLE) must first be calculated:[274]

---

[269] It is contended by Appelgate, McFarlan and McKenney (n 12) 241 that the following steps may be taken to safeguard information being held on a single site:

(i) "Limit physical access to the computer room;
(ii) Surround the data center with chain-link fences, automatic alarms and dogs;
(iii) Monitor access to inner areas by guards using remote TV cameras;
(iv) Ensure an uninterrupted power supply, including banks of batteries and stand-alone generators;
(v) Using a Halon inert gas system to protect the installation in case of fire;
(vi) Complex, encrypted access codes that serve to deny file and system entry to unauthorised personnel to the network;
(vii) Storing a significant number of files off-site and updating them with a high level of frequency; and
(viii) Use rigorous procedures for both certifying new programs and change in the existing programs."

[270] (n 11) 14.
[271] ibid.
[272] (n 11) 15.
[273] (n 48) 249.
[274] ibid.

Asset value	x	Exposure factor	=	Single loss

Rather than using highly technical jargon, threats need to be translated into understandable business terms, as it is important that those people entrusted with the decision-making of the organisation fully comprehend the magnitude of the threat facing the organisation.[275] It is recommended that managers, users, as well as information systems practitioners are made fully aware of the potential threats facing the organisation, possible consequences that may ensue if the threats materialised, as well as steps that need to be taken to minimise the risk.[276] Only if all key role players understand the nature of the risk will they be able to combat it.

Result delivered by phase 2: Drafting of a threat statement consisting of a comprehensive list of identified threat-sources, the motivation behind the threats and threat actions specifically relevant to the organisation. [277]

Phase 3: Vulnerability identification

Goal: Compile a list of system vulnerabilities that may be exploited by the threat-sources identified in phase 2. [278]

Vulnerability identification may be viewed as encompassing:

[275] (n 152) 2.
[276] (n 152) 4.
[277] (n 40) 15.
[278] ibid.

"the qualitative identification of assets, both tangible and intangible, their replacement costs, and the further valuing of information asset availability, integrity and confidentiality. These value(s) may be expressed in monetary (quantitative) or nonmonetary (qualitative) terms." [279]

(i) Attack methodology:

(a) A vulnerability is discovered or postulated and discussed on the Internet amongst, for instance fellow hackers; [280]

(b) An individual or group of individuals develop a code/tool that may be used to effectively exploit the vulnerability, and then release this code/tool; [281]

(c) Initial attempts are made by hackers to "test the waters" at which time they mostly use unrefined methods and tools;[282]

(d) After a short lapse of time the unrefined tool or method is refined, made more sophisticated, user-friendly and effective. [283] After this process have been completed the tool or method is made available on the Internet; and

(e) The newly developed tool or method augments as it gains acceptance and popularity amongst the hacker population. [284]

(ii) Factors that may impact on the level of vulnerability include:

(a) Sensitivity of information generated, stored, processed or used by the organisation; [285]

---

279 (n 48) 255.
280 (n 152) 9.
281 ibid.
282 ibid.
283 ibid.
284 ibid.
285 (n 11) 15.

(b) The question whether employees have received emergency training on how to respond to a security incident; [286]

(c) The presence of detective and preventative security measures;[287]

(d) Employee's attitude towards security issues, as well as satisfaction levels regarding their working environment. In a large number of security incidents the threat agent would usually be a disgruntled employee; [288]

(e) The level of training provided to employees; [289]

(f) Prominence of the organisation (Is it a well-known, high profile company?); [290]

(g) The question whether written, widely understood policies, guidelines and procedures are in place, and are made known to all; [291]

(h) History of how the organisation dealt with security incidents in the past (Was it swept under the rug, or reported to, and handed over to the appropriate authorities?); [292] and

(i) The economic environment which encircles the organisation. [293]

It is recommended by the NIST [294] that the identification of vulnerabilities will comprise of the following 3 processes:

(a) Make use of a vulnerability source; [295]

(b) Develop a security requirement checklist; [296] and

(c) Perform **system security testing**. [297]

---

286 ibid.
287 ibid.
288 ibid.
289 ibid.
290 ibid.
291 ibid.
292 ibid.
293 ibid.
294 (n 8) 16-19.
295 (n 40) 16.
296 ibid.
297 ibid.

One area of specific importance under **system security testing** is **penetration testing**.[298] **Penetration testing** is a popular and effective method used by organisations, which allows designated individuals to try and "hack" or "break into" the organisation's computer systems. These individuals are usually encouraged to use state-of-the-art, sophisticated hacking techniques and tools in order to complete their mission. The effectiveness of this type of testing lies in the fact that previously unknown or unacknowledged vulnerabilities are detected and dealt with.

Penetration testing may be defined as "…a formalized set of procedures designed to bypass the security controls of a system or organization for the purpose of testing that system's or organization's resistance to such an attack."[299] It is contended by Tipton and Krause[300] that penetration testing "attempts to gain access through available vulnerabilities by taking on the mindset of the perpetrator." There are 3 requirements that must be met for penetration testing to be successful, namely:

(i) "Test must have a defined goal and that goal should be clearly documented;
(ii) The test should have a limited time period in which it is to be performed; and
(iii) The test should have the approval of the management of the organization that is the subject of the test."[301]

The development of the system vulnerability checklist will normally address 3 security areas, namely:[302]

---

[298] It is important to bear in mind that although penetration testing is an invaluable tool for organisations to identify security vulnerabilities, this same tool may be used by hackers and crackers to identify and exploit security weaknesses existing within the organisation's computing environment. Tipton and Krause (n 186) 201. Various forms of penetration testing exist. Three principal tests are encountered:
(i) Level 1: Zero-knowledge penetration testing. The "attacker" has no prior knowledge of the system architecture he/she is attempting to infiltrate. The attack is launched from an internal source;
(ii) Level 2: Full-knowledge penetration testing: the "attacker" has a comprehensive knowledge of the network architecture he is attempting to infiltrate. The attack is launched from an external source; and
(iii) Level 3: Internal penetration testing. This assault on the network security is launched from inside the organisation Tipton and Krause (n 186) 557.

[299] (n 186) 201.

[300] (n 186) 557.

[301] ibid.

[302] The diagram that follows is based on a framework developed by the NIST (n 40) 18-19.

(i) Management; [303]

(ii) Operational; [304] and

(iii) Technical. [305]

Security area	Security criteria
Management security	(a) Assignment of responsibility (b) Continuity of support (c) Incident response capability (d) Periodic review of security controls (e) Personnel clearance and background investigation[306] (f) Risk assessment (g) Security and technical training (h) Separation of duties (i) System authorisation (j) System application security plan
Operational security	(a) Control of air-born contaminants (b) Controls to ensure the quality of the electrical power supply (c) Data media access and disposal (d) External data distribution and labeling (e) Facility protection (f) Humidity control (g) Temperature control (h) Workstation, laptops, and stand-alone personal computers
Technical security	(a) Communications (b) Cryptography (c) Discretionary access control (d) Identification and authentication (e) Intrusion detection (f) Object reuse (g) System audit

303 (n 40) 18.

304 ibid.

305 (n 40) 19.

306 Background checks represent a method by which the organisation can protect itself against an internal threat. In the United States of America organisations in approximately thirty states can be held legally liable of **negligent hiring.** This form of liability entails that an employer can be held liable for actions his employee performed after-hours if the firm could have prevented the act had they known about his past offences. This form of liability extends the scope of vicarious liability to a whole new level. In accordance with vicarious liability an employer may be held vicariously liable for the actions of his employee, provided that the employee was acting within the scope of his employment. The leading case in South Africa on vicarious liability is *Magna Alloys and Research (SA) (Pty) Ltd v Ellis* 1984 (4) SA 874 (A). The liability for negligent hiring may have far-reaching implications for employers, therefor top management and directors. A customer who has suffered damages due to for instance, credit card fraud may potentially collect such damages from the employer himself, if a background check would have revealed that the employee had a criminal record. Greenstein and Vasarhelyi (n 255) 230.

Result delivered by phase 3: a comprehensive list of system vulnerabilities that may be exploited by the threat-agent. [307]

Phase 4: Likelihood determination [308]

"Risks can be classified in terms of their likelihood of occurrence and the level of their impacts." [309]

Goal: to determine the likelihood that the vulnerability will be exploited. [310]

The likelihood of a vulnerability being exploited will depend on the interplay between the following factors:[311]

(i) The threat-source, its motivation and its capabilities; [312]

(ii) Nature of the vulnerability; [313] and

(iii) Existence and effectiveness of current controls that are in place. [314]

307 (n 40) 19.

308 The terms "likelihood" and "probability" are often used interchangeably in this context. Probability may be defined as: "…the chance or likelihood, in a finite sample, that an event will occur or that a specific loss value will be attained should the event occur…" Tipton and Krause (n 48) 251.

309 (n 23) 106.

310 There exist a direct correlation between the likelihood that a vulnerability will be exploited and the threat itself. For instance, if the organisation is dealing with a natural threat research may be done into the likelihood of occurrence by contacting the weather service in the place where the organisation is situated, and reviewing their past, present and predicted findings. If the organisation is faced with any of the other types of additional threats, more intensive research will be required. For instance crime statistics may be analysed, documented threats that the organisation has been faced with in the past must be considered. The organisation may also rely heavily on the findings of its internal and external auditors. Insurance companies may furthermore be contacted to obtain a clear picture of what they regard as being a serious threat in the organisation's operational environment. Peltier (n 11) 15-16. The process of likelihood determination therefor requires research into various sources of information. Amongst these sources we find historical records, past experience, checklists, similar projects, brainstorming, published literature, industry best practice, expert commercial and technical judgements, and relevant published materials Bowden , Lane and Martin (n 15) 12-13.

311 (n 8) 21.

312 (n 40) 21.

313 ibid.

314 ibid.

Likelihood definitions as developed by the NIST:[315]

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

Result delivered by phase 4: ranking the likelihood that vulnerability may be exploited (high, medium and low). [316]

Phase 5: Impact Analysis [317]

Goal: To determine what would be the result if a threat successfully exploits vulnerability. [318]

The term "impact" reflects the "degree of harm and is concerned with how significant the problem is, or how much effect it will have on the organisation."[319]

This step is dependent on clarity and certainty regarding the following issues:

(i) The level of security required to ensure that data integrity, confidentiality and availability are not compromised, therefor clarity regarding the sensitivity of the information; [320]

(ii) Functions performed by the IT system; [321] and

(iii) Importance of these systems for the organisation. [322]

---

315 ibid.
316 ibid.
317 It is contended by Tipton and Krause (n 186) 280 that the most difficult part of any risk assessment process is to "…determining the potential impact and the realistic chances of the event occurring...".
318 (n 40) 21.
319 (n 186) 555.
320 (n 40) 22.
321 (n 40) 21.
322 ibid.

Quantitative and Qualitative risk assessment: At present various models and methods exist to assess the risks facing organisations.[323] Risk assessment is generally divided into 2 principal categories or approaches, namely:

(i) Quantitative risk assessment; and

(ii) Qualitative risk assessment. [324]

Result delivered by phase 5: is the calculation of the estimated impact (high, medium or low). [325]

Phase 6: Control recommendations [326]

Goal: identify controls that would effectively reduce, minimise or eliminate the risks previously identified.[327]

The selection of corrective action will mostly be based on 2 factors, namely: (i) the cost involved; [328] and (ii) the effectiveness of the control. [329]

This step will therefor identify possible countermeasures that may be taken to reduce or mitigate the risk while simultaneously being cost-effective. It must be ensured that the cost of implementing the countermeasures does not outweigh the cost of the actual threat realising. [330] It is recommended that the designated individual or group responsible for making the recommendation investigate all possible alternatives before selecting control(s) to be implemented.

---

323 (n 11) 19.

324 See Annexure J for a better understanding of the inherent differences between quantitative and qualitative risk assessment.

325 (n 40) 23.

326 Step six represents the second component or "building block" of the risk management process. It will therefor be discussed in greater detail later in this chapter under the heading "risk mitigation."

327 (n 40) 26.

328 (n 40) 25.

329 ibid.

330 ibid.

Control objectives and their corresponding safeguards: [331]

Control	Safeguards
Avoidance (a) Proactive controls (b) Goal is to minimise risk of threat materialising	(a) Encryption (b) Authentication (c) System security architecture (d) Information awareness program (e) Public key infrastructure (f) Policies and standards (g) Information security program (h) Facilitating risk assessment process
Assurance (a) Controls provide a positive declaration that existing safeguards and controls are functioning at maximum capability and efficiency	(a) Penetration testing (b) Vulnerability assessment (c) Standards testing (d) Application security review (e) Perimeter testing
Detection (a) These controls ensure the early detection, interception and response to a security incident	(a) Intrusion detection [332]
Recovery (a) Controls restore the environment as it was before and examines the cause of the security incident	(a) Business continuity plan (b) Business impact analysis (c) Disaster recovery plan (d) Investigation tools (e) Crisis management planning (f) Incident response procedure

The following questions may proof helpful in order to decide if the potential risk should be reduced, mitigated, avoided, transferred or accepted:

---

331 The diagram depicted was advanced by Peltier (n 11) 30.

332 Tipton and Krause (n 48) 683 define intrusion detection as: "…the process of discovering unauthorised use of computers and networks through the use of software designed for this purpose...". It is important to bear in mind that intrusion detection does not address a specific risk, as one would find with encryption or third-party authentication. The result of this is that intrusion detection is often overlooked as a viable option. Intrusion detection and monitoring systems will provide the organisation with the following benefits:

(i) "protected information is not accessed by unauthorised parties, and if it is, there is a clear audit record;
(ii) the ability to monitor network traffic without impact to the network;
(iii) actively respond to attacks on system;
(iv) information security organisations understand the attacks being made and can build systems and networks to resist those attacks; and
(v) metrics reporting is provided" Tipton and Krause (n 186) 584-585.

(i) Which steps may be taken to address unacceptable risks?; [333]

(ii) What will be the cost associated with these steps?; [334]

(iii) Will the controls and safeguards that were decided on be effective?; [335] and

(iv) What would the residual risk be? [336]

Result delivered by step 6: the selection and consideration of different types of control measures to reduce the risk to an acceptable level.

Phase 7: Result documentation

"The value of risk assessment will be judged by how well it is presented to management."[337]

Goal: drafting of a risk assessment report that gives a brief, yet thorough overview of the risk, threats and vulnerabilities facing the organisation, the likelihood that they will materialise or be exploited, and the decided upon control measures/safeguards to be implemented.

After the risk assessment process has been completed a **Risk Assessment Report** [338] must be compiled that will give an overview of:

(i) Threats and vulnerabilities identified; [339]

(ii) Measurement of the risk; [340] and

(i) Recommended controls to be implemented. [341]

---

333 (n 152) 33.
334 ibid.
335 ibid.
336 ibid.
337 Hamilton "New trends in risk assessment" (April 1995) *Data Security Management AIMS* 21.
338 See Annexure K for a sample risk assessment report.
339 (n 40) 26.
340 ibid.
341 ibid.

This Risk Assessment Report is in congruence with the recommendation made by the King II report. King II requires of organisations to systematically document the risk assessment process as well as the results delivered by this process and communicate this information to all relevant role-players.[342] This report must ultimately form part of a database that the organisation must construct. This database should be used to justify past, present and future decisions and acts. It will also act as proof that due diligence have been performed.[343]

King II requires of the risk assessment process and report to reveal and contain, at minimum, information on the following:

(i) An estimate of the likelihood of occurrence;[344]

(ii) Quantification of the probable impact; [345] and

(iii) Comparison to available benchmarks. [346]

It should be kept in mind that after top management have received the recommendations made by the team they will have to act on it and determine if the risk should be deemed acceptable or unacceptable. If it is decided not to implement corrective action as recommended, this decision must be fully motivated and explained in writing.[347]

Ultimately, the importance of the result documentation phase lies therein that it enables the organisation to start building a database of threats, risks and vulnerabilities that the organisations have been faced with in the past, are faced with in the present, and might be faced with in the future. [348] The essence of a database is best captured by the age-old expression "history repeats itself", as the majority of security incidents and/or breaches still result from common security vulnerabilities that the organisation has neglected to

---

342 (n 35) 78.
343 (n 11) 32.
344 (n 35) 76.
345 ibid.
346 ibid.
347 (n 149) 26.
348 Boespflug, Neal and Crowe "Secure your systems now: just one hacker can wreck your business" (last visited 18 April 2002) http://www.itweb.co.za 3.

address. [349] Hackers are known to take advantage of "the easiest and best-known opportunities first." [350]

Result: delivered by step 7: a comprehensive document containing a summary of the radius of risk to information security in the organisation.

After completion of steps 1-7 the following information will be available to the organisation:

(i) "A brief description of the risk event;
(ii) The possible cause and consequences for each feasible event;
(iii) The main phase of the project or business activity in which the risk is most likely to occur;
(iv) The critical success factors likely to be affected if the risk occurs;
(v) An analysis of the likelihood of occurrence of the risk;
(vi) Its impact if it does occur; and
(vii) The position or department responsible for managing the risk." [351]

The question may be asked which risk assessment process will reveal itself to be the most effective for an organisation. [352] Various risk assessment methods, products, software and consulting services exist that may aid organisations wishing to perform risk assessment. No one of these methods may however be said to be the correct approach to risk assessment. The answer to this question will therefor lie with the organisation itself, as it will be the only one who can determine which method, product, tool or software will accomplish the desired result. It is therefor recommended that organisations take the time to investigate various methods and processes before deciding on one or more to utilise. A static approach to risk assessment will never be acceptable. For risk assessment to

---

349 ibid.
350 ibid.
351 (n 15) 13.
352 Examples of these may include: vulnerability analysis (investigates and analyses the vulnerabilities faced by a department based on the people working in that department, therefor taking into account skills required, working conditions and nature of job), hazard analysis (analyses the hazards that a site is most susceptible to), threat analysis (analyses how the threat, if materialised will impact on certain business processes), single-time algorithm (combines elements of quantitative as well as qualitative risk assessment results to create a mathematical formula).

succeed a real-time, up-to-date and accurate assessment and response is needed to face potential threats head-on.[353]

6.3.2.8.7 Benefits inherent to risk assessment

The following benefits will be derived from a successful risk assessment process:

(i) Assurance that the greatest risk have been identified and addressed;

(ii) Increased understanding of risks amongst employees;[354]

(iii) Mechanism for reaching consensus on issues pertaining to:

  (a) Which risk(s) presents the greatest threat? [355]

  (b) How should this risk be approached, reduced and/or mitigated?[356] and

  (c) Should the risk(s) be mitigated or reduced at all, or is the organisation prepared to accept the risk. [357]

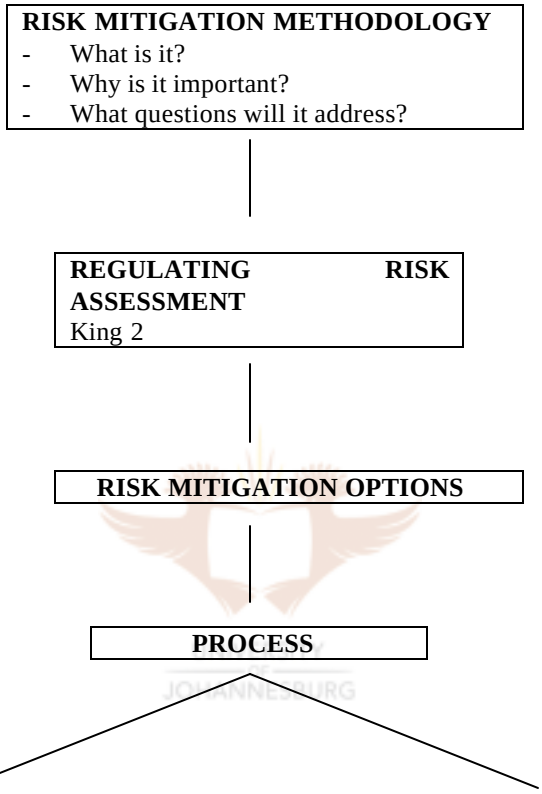
(iv) Support for needed controls; [358] and

(v) Means for communicating results.

[353] (n 152) 5.
[354] (n 15) 234.
[355] (n 149) 18.
[356] ibid.
[357] ibid.
[358] (n 152) 33.

6.3.2.9 PHASE 2: RISK MITIGATION

ROADMAP TO RISK MITIGATION



CONTROL IMPLEMENTATION	CONTROL CATEGORIES
Step 1: Prioritise actions Step 2: Evaluate recommended controls Step 3: Conduct cost-benefit analysis Step 4: Select control Step 5: Assign responsibility Step 6: Develop a safeguard implementation plan Step 7: Implement selected controls	1. Technical security controls: (a) Support (b) Preventative (c) Detect and recover 2. Management security controls: (a) Preventative (b) Detection (c) Recovery 3. Operational security controls: (a) Preventative (b) Detective

6.3.2.9.1 Risk mitigation methodology

By gaining a clear understanding of the business risks attached to information security, through risk identification, evaluating and impact analysis, the first component/phase of the risk management life cycle has been completed. Risk mitigation represents the second component/phase of the risk management process, and comprises of the prioritisation, evaluation and implementation of control mechanisms and safeguards as identified and recommended in the risk assessment process.[359]

(i) Risk mitigation defined

Risk mitigation may be defined as "(t)he process of taking specific causes of action to reduce the probability/or reduce the impact of the risk."[360]

(ii) The need for risk mitigation

As stated earlier risk is an inherent consequence of doing business. The elimination of risk is therefor a fantasy. Through the process of risk mitigation it is expected of business managers to find the most efficient, cost-effective safeguard or control to reduce the risk to an acceptable level, while simultaneously placing the smallest possible impediment on the organisation's resources.[361]

(iii) Risk mitigation will address the following questions:

(a) What can be done? (risk mitigation); [362]

---

[359] (n 40) 27.
[360] (n 213) 42.
[361] (n 40) 27.
[362] (n 48) 248.

(b) How much will it cost? (annualized);[363] and

(c) Is it cost effective? (cost / benefit analysis). [364]

6.3.2.9.2 Risk mitigation options

The following risk mitigation options are at the disposal of the organisation:[365]

(i) Risk assumption / acceptance

Risk acceptance may be defined as "…that risk which the company is knowingly prepared to accept…",[366] it is "the decision to acknowledge and endure the consequences if a risk event occurs."[367] If it is decided by the designated individual or group that the risk should be accepted, it is recommended that this person/group prepares a **Risk Acceptance Statement** (waiver) which should include the following information:

(a) Why the risk is deemed acceptable; [368]

(b) Detailed description of the risk, as well as losses suffered or damages that may be incurred if the risk materialises;[369] and

(c) Alternatives to reduce or mitigate the risk, and the costs involved.[370]

It should be kept in mind that the person/group who signs the risk acceptance statement will be held accountable for his/their decision. [371] The risk acceptance statement will generally be encountered where a deviation or non-compliance with a set standard

---

363 ibid.
364 ibid.
365 (n 40) 27.
366 (n 186) 555.
367 (n 213) 43.
368 (n 149) 33.
369 ibid.
370 ibid.
371 (n 149) 34.

occurs. This statement still needs to be approved on a higher level, and will generally only be valid for a period of six to twelve months.[372]

Risk acceptance may come to the fore in two ways, namely active and passive risk acceptance. [373] Passive acceptance may be viewed as embodying "the acceptance of risk without taking any action to resolve it or otherwise manage it." [374] The only task that would have to be performed under this form of acceptance is the formal documentation by directors and top management acknowledging that they are aware of the fact that this risk exists, and that they deem it to be an acceptable risk. [375] With active risk acceptance the task of acknowledgement of risk, as set out above must also be performed, but in addition to this task, contingency plans[376] are developed. [377]

Reasons that may be advanced that would make the potential risk acceptable:

a) Cost of potential loss may be very low;
b) Probability of the risk/loss materialising could be very low; or
c) Potential loss may be covered sufficiently by insurance.

(ii) Risk avoidance

Risk avoidance may be defined as a "…risk response strategy that eliminates the threat of a specific event, usually by eliminating its potential cause."[378] It therefor entails eluding the risk in its entirety (threat-agent, motivation and impact) by, for instance shutting down the system when a risk is identified. [379]

---

372 ibid.
373 ibid.
374 ibid.
375 ibid.
376 Pritchard (n 213) 310 defines a contingency plan as: "…a plan that identifies alternative strategies to be used if specified risk events occur…". For practical guidance on contingency planning, consult Myers *Managers' Guide to Contingency Planning for Disaster* (1999).
377 (n 213) 43.
378 (n 213) 308.
379 (n 8) 27.

It is contended by Hunter[380] that risk avoidance is impossible. He argues that the financial resources divulged by such an approach to information security would be disproportionate to the risk it is attempting to address. The resource investment, in the form of time and skilled personnel, required by such an approach will be impractical and will lead to impossible demands being placed on such resources. [381]

(iii) Risk limitation

Risks may be limited by introducing effective controls that would reduce the impact if the risk materialised. [382]

(iv) Risk planning

This would involve the design of a risk mitigation process that would prioritise, implement and maintain controls. [383]

(v) Risk transference[384]

Risk transfer may be viewed as an attempt by the organisation to "shift" responsibility for the threat to a third party.[385] The risk is therefor transferred to, for instance an insurance company, by securing compensation in the event of a threat materialising or a vulnerability being exploited by paying a premium on a periodical basis.[386] Risk transfer

---

380 (n 152) 29.
381 ibid.
382 (n 8) 27.
383 ibid.
384 Risk transfer is also referred to as risk deflection Pritchard (n 213) 42.
385 (n 213) 42.
386 Keep in mind that computer hardware is usually easily insured, whereas data is not. Organisations will only be able to obtain insurance for the cost of data recovery.

may be considered as a viable option when the proposed security measures would result in an impractical and costly exercise. [387]

Keep in mind that through risk transfer the likelihood of a risk materialising has not been eliminated or even reduced.[388] Risk transfer will only ensure that the organisation is compensated to a certain extend for the damages or losses suffered. [389] Responsibility for the risk itself has however not been delegated. [390]

The question of which option(s) will be utilsed by an organisation is very subjective and will depend on for instance, the organisation's mission and goals, the controls which have been implemented, and its information security environment.[391] It is important that the organisation consider all possible alternatives before deciding on one or two options.

6.3.2.9.3 Risk mitigation strategy

A risk mitigation strategy will provide an answer to the following question: when and under which circumstances should the organisation act?

To determine whether or not control actions should be implemented the following process may be followed:[392]

---

387 Risk transfer may take various forms ranging from insurance policies, the pooling of risks, to hedging Wixley and Everingham (n 9) 82.

388 (n 48) 247.

389 ibid.

390 (n 213) 42.

391 (n 40) 27.

392 The framework that is proposed here is based on the "Risk Mitigation Action Plan" as discussed by the NIST (n 40) 28.

Determine the following:

1. Does a threat-agent/source exist?	**2. Does a risk exist?**	**3. Does a vulnerability exist in the system, application or program.**

If the answer is **"yes"** to **all three** of these questions determine the following:

Is the cost the attacker has to incur < than the gain he will receive?

If the answer is "**yes**"

Determine if the loss anticipated > than the threshold.

If the answer is "**yes**"

The organisation is faced with an unacceptable risk.

The risk mitigation strategy involves "the selection of one or more risk treatment options, which collectively will reduce the overall risk exposure of the project or business to an acceptable level."[393]

Keep in mind that sometimes there will not be a need for action, or at very best little action. Taylor[394] quite correctly observe that with risk mitigation, as with most things in life "the key is to know when to act and (often more importantly) when not to act."

6.3.2.9.4 Risk mitigation in the light of King II

The King II report recommends that a comprehensive system of controls should be implemented by the board in order to mitigate risks, and reduce the possibility that they will be realised to the lowest possible level.[395] The report therefor recognises the importance of risk mitigation within the risk management context.[396]

It is furthermore acknowledged that there are certain risks that do not justify the costs that will have to be incurred in order to control them. This realisation is accompanied by a solution in the form of internal controls. Internal controls may be used as an effective method to mitigate certain risks by reducing it to an acceptable level. [397]

---

393 (n 15) 93.
394 Taylor "Forewarned is forearmed: the laws of IT can make or break a system" (last visited 18 April 2002) http://www.itweb.co.za 2.
395 (n 35) 81.
396 (n 35) 73.
397 (n 35) 73-74.

Internal controls[398] may be defined as:

> "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> (i) Effectiveness and efficiency of operations;
>
> (ii) Reliability of financial reporting; and
>
> (iii) Compliance with applicable laws and regulations."[399]

The report contents that internal controls will help the organisation gain positive assurance that it is meeting its set goals, objectives and mission, by focussing, and re-assuring the organisation of the following:

(i) "Safeguarding of the company's assets;
(ii) Supporting business sustainability under normal as well as adverse operation conditions;
(iii) Reliability of reporting; and
(iv) Behaving responsibly towards stakeholders."[400]

The report recommends that internal controls form part of the daily activities of the organisation, and that its appropriateness and effectiveness are reviewed on a regular basis.[401] The essence of internal controls are embedded in policies and procedures that ensure management's plans are implemented. [402]

---

398 Examples of internal controls would include, but are not limited to approval of transactions, authorisation powers, reconciliation or verification of records, review of operating performance, ensuring security of assets and segregation of duties. Wixley and Everingham (n 9) 83.
399 (n 9) 83.
400 (n 35) 73-74.
401 (n 35) 80.
402 (n 9) 83.

6.3.2.9.5 Control implementation [403]

Control implementation would involve the following activities:

Step 1: Prioritise actions

As a result of the already completed risk assessment report, implementation actions should now be prioritised. [404] It stands to reason that those risks that were categorised as unacceptably high should receive immediate and thorough attention. [405] "The options that are selected depend on the degree of control of treating the identified risks. The greater level of control, the more likely the risks will be treated using proactive measures."[406]

Result delivered by this step is the ranking of actions from high, medium, to low. [407]

Step 2: Evaluate recommended control options

In this step attention is focused on the recommended controls to be implemented. [408] This would require a thorough investigation into the "appropriateness, effectiveness and feasibility involved with the implementation of such a control", [409] keeping in mind the security environment in which it is expected to function. [410]

Result delivered by this step is a list of practical and manageable controls. [411]

---

403 Jeynes *Risk Management: 10 Principles* (2002) 62 defines control as: "…an action/device/strategy intended to eliminate/alleviate/reduce the negative impact on the business or individual of a situation or event...".
404 ibid.
405 ibid.
406 (n 15) 93.
407 (n 40) 29.
408 ibid.
409 ibid.
410 ibid.
411 ibid.

Step 3: Conduct Cost-Benefit Analysis (CBA)

To decide on the issue of cost-effectiveness of a control, it is recommended that managers conduct a cost-benefit analysis. [412]

The cost-benefit analysis could be qualitative or quantitative in nature. The aim with this exercise is to express in monetary terms, and justify the resource investment in the development and implementation of recommended, and finally decided on control measures by indicating the reduction in the level of risk that would result. [413] Ultimately the cost-benefit analysis will result in a better return on investment (ROI) for shareholders, as it enables the organisation to find an equilibrium between the value of an asset and the cost associated to protect it. [414]

The cost-benefit analysis will entail the following:

(i) An investigation into what the results would be if new or more sophisticated controls were to be implemented. [415] These results are compared to what the position would be if the organisation abstained from implementing new or improved controls. [416]

(ii) Calculate what expenditure must be incurred in order to implement the control, by for instance asking the following questions:

(a) Does the organisation have to purchase new hardware and/or software?

(b) What maintenance costs are attached to the controls?

(c) Does this control require of personnel to undergo further training?

(d) Does the organisation need to redraft existing security policies and procedures?

(e) Does the implementation of the controls require outsourcing?

---

412 (n 40) 35. The concept of cost-benefit analysis is usually associated with the following catch phrase "getting more bang for your buck".

413 Hester and Harrison (ed) *Risk Assessment and Risk Management* (1998) 26.

414 (n 337) 10.

415 (n 40) 35.

416 (n 40) 37.

(iii) Ultimately the cost of implementation of the new or improved control must be weighed against the impact or cost that will be incurred/suffered if the organisation's information assets are corrupted, modified, damaged, altered, lost, destroyed or unavailable. [417]

The following simplistic representation of a cost-benefit analysis may be advanced to illustrate the purpose of such an exercise:[418]

Expected Loss = P1 x P2 x L

P1: Probability of attack;[419]

P2: Probability of attack being successful; and

L: Loss that may be incurred if attack is successful.

The result representing the expected loss should now be compared to cost of implementing the safeguard or control. [420]

Result delivered by this step is to give managers an idea of what it will cost to implement the recommended controls, as well as what the cost would be if they decide not to do so.[421]

Step 4: Select control

At this point in the process managers should have enough information to make an informed decision regarding whether or not to implement a control, and which control(s) to implement.[422]

---

417 (n 40) 38.

418 Turban, McLean and Wetherbe *Information Technology for Management: Making Connections for Strategic Advantage* (1999) 680-681.

419 Calculating the threat occurrence rate is an essential part of the cost-benefit analysis process Hamilton (n 337) 10.

420 (n 413) 680-681.

421 (n 40) 39.

422 (n 8) 29.

Result of this step is the selection of control(s). [423]

Step 5: Assign responsibility

Assign responsibility for the implementation as well as monitoring of the controls by taking into account which personnel possess over the necessary skills and expertise.[424]

Step 6: Develop a safeguard implementation plan

Step 7: Implement selected controls

Result of this step is residual risk. [425]

Residual risk may be defined as "…that which remains beyond the identified, managed risks. An organisation's risk acceptance is determined by how much residual risk it is prepared to carry."[426] It therefor represents the risk remaining after the implementation of new or enhanced controls.[427]

6.3.2.9.6 Control categories [428]

It is recommended by the NIST [429] that organisations consider technical, management and operational controls when implementing the recommended controls.

Due to the highly technical nature of this part of the discussion, control categories are not going to be discussed comprehensively.

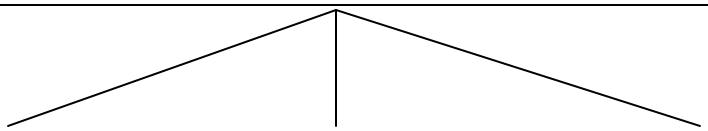
---

423 ibid.
424 (n 8) 30.
425 ibid.
426 (n 15) 6.
427 (n 48) 111.
428 Countermeasure or control categories generally comprise of three parts which work in tandem, namely (i) protection/prevention; (ii) detection; and (iii) reaction Schneier *Secrets and Lies* (2000) 279.
429 (n 40) 32-37.

Technical controls

(a) Technical Security Controls will usually involve system architecture, engineering principles and security packages.[430]

(b) Technical Security Controls may be subdivided into the following categories:



Support Controls	**Preventative Controls**	**Detect and Recover Controls**
- These controls form the basis for the implementation of other controls. They are not specific, and underline most IT capabilities.[431] - Support controls would include: identification, cryptographic key encryption, security administration and system protection.[432]	- These controls focus on preventing security breaches from occurring in the first place.[433] - These controls would include, but are not limited to: (a) Authentication[434] (b) Authorisation[435] (c) Access Control[436] Enforcement[437] (d) Non-repudiation[438] (e) Protected Communications[439] (f) Transaction Privacy[440]	- These controls focus on detecting and recovering from security breaches.[441] - **Detection Controls** serve as to discover the presence or existence of a transgression or attempted transgression.[442] - **Recovery controls** regain use or control over lost computer resources.[443] - Both controls would include: audit, intrusion detection and containment, proof of wholeness, restore secure state, virus detection and eradication.[444]

430 (n 40) 32.
431 (n 40) 33.
432 ibid.
433 (n 40) 31.
434 (n 40) 34.
435 ibid.
436 ibid.
437 ibid.
438 ibid.
439 ibid.
440 (n 40) 35.
441 ibid.
442 ibid.
443 ibid.
444 ibid.

Management security controls These controls center around procedures, policies and guidelines that must be adhered to in order for the organisation to reach its set objectives.[445]		
Preventative Management security controls[446]	Detection management security controls[447]	Recovery management security controls[448]

Operational security controls These controls are used to address weaknesses that may be exploited by the threat agent.[449]	
Preventative Operational Controls[450]	Detection Operational Controls[451]

6.3.2.10 Risk management - a continuous process

Organisations should not adopt a static approach to information security risk management, but rather see it for what it is: dynamic, complex and ever changing. The time that lapse between when a vulnerability is first detected and when it is being exploited is decreasing by the minute. It is interesting to observe that the issue of urgency and real-time reaction to threats are widely acknowledged within the context of viruses, yet other threats, which are found just as abundantly, are widely ignored. It should be kept in mind that as the organisation grows and expands it will be necessary to update software applications and component, changes in personnel and security policies are also bound to occur.[452] The result of this is that every change inevitably brings with it new threats, vulnerabilities and risks waiting to be discovered and exploited.[453] Risk management is therefor a continuous process that needs to keep on evolving. [454]

---

445 ibid.
446 ibid.
447 ibid.
448 ibid.
449 ibid.
450 ibid.
451 ibid.
452 (n 48) 248.
453 ibid.
454 (n 255) 257.

The King II report also acknowledges that risk management is a continuous process. It suggests that the "health" of an organisation's computer systems, applications and networks should be monitored on a continuous basis. This process would include the following:

(i) Continuous monitoring of the computer system, network and application of the organisation; [455]

(ii) Remain informed about new risk, threats and vulnerabilities as they are discovered; [456]

(iii) Perform penetration testing; [457]

(iv) Risk assessment should be performed on an annual basis; [458]

(v) Reports on, and review of the risk management process should be performed on a regular basis; [459]

(v) Assess the appropriateness of existing policies, standards, guidelines and controls that have been implemented, as well as the rate of compliance with the aforementioned; [460] and

(vi) Promote awareness and educate employees on issues pertaining to information security on a continuous basis. [461]

6.3.2.11 Conclusion

"Risk is woven into the very fabric of life, and although risk can never be completely mastered, it can be managed."[462]

The concept of risk assessment and management is not alien to organisations. They have been dealing with it for quite some time now especially within the financial arena. The

455 (n 35) 76.
456 ibid.
457 ibid.
458 ibid.
459 ibid.
460 ibid.
461 ibid.
462 ibid.

newest risk area, information security risk management and assessment do however represent uncharted waters for most organisations. Organisations are experiencing far greater risks than ever before, because of the convergence of the following factors: (i) interconnectivity (connectivity results in organisations no longer having control over who has access to its information. It creates multiple points of entry against which cyber attacks may be launched); (ii) the fact that information is more easily accessible than ever before; and (iii) the reality that risks are constantly changing at an alarming, ever-increasing rate.

Although it is acknowledged that information security is not the only risk area facing organisations, it is one of the most important risk areas, as organisations rely heavily on the integrity, availability and confidentiality of information. Organisations will therefor have to pay serious attention to issues surrounding information security and the risks unique to the information assets of the organisation. [463]

The introduction of the recently issued King II Report on Corporate Governance as well as the increasing demand to demonstrate good corporate governance are some of the drivers that make risk management in the information security arena of pivotal importance, not only for the continued survival of the company, but also for the continued existence of the board of directors. Through an effective process of risk management the board will be able to discharge their responsibility of due diligence.

Shareholders are demanding of the board and top management to manage these risks by:[464]

(i) Ensure that there is **transparency** about the risks, threats and vulnerabilities to which the organisation might fall prey;

(ii) Acknowledge that the final **responsibility** for IT risk management does not lie with the IT department, but rests firmly in the hands of the board (the days of using IT personnel as scapegoats are over);

---

[463] (n 33) 2.

[464] IT Governance Institute "Board briefing on IT governance" (last visited 27 July 2002) http://www.Igovernance.org 23.

(iii) Understand that even though the initial resource investment in the development and implementation of an effective and efficient risk management program will seem enormous, it will result in **numerous benefits** for the organisation, such as an increase in its competitive advantage, customer confidence and shareholder value;

(iv) Risk management is not a once-off process, but a **continuous** journey that needs to be re-visited on a regular basis;

(v) Risk management must be seen as an **inseparable part** of the business process and must at all times support the business objectives and mission;[465] and

(vi) A holistic and proactive approach to risk management must be adopted as this will enable the organisation to obtain a sustainable **competitive advantage.**[466]

OUTCOMES DELIVERED BY STEP 2:

(i) The complex and multifaceted nature of risk management is appreciated, acknowledged and understood;

(ii) It is recognised that the ultimate responsibility for risk management is vested in the board.[467] Although the board is allowed to delegate certain functions pertaining to the risk management to designated role-players, they are not allowed to delegate their responsibility for this process; [468] and

---

[465] (n 11) 3.
[466] Retief "Managing risk in commodity training" (last visited 15 August 2002) http://www.itweb.co.za 1.
[467] (n 35) 75.
[468] ibid.

(iii) It is recognised that management is answerable to the board for the practical design, implementation, monitoring and evaluation of the risk management process. [469]

"To tire of risk is to tire of life."[470]

[469] ibid.
[470] (n 20) ix.

IN SUMMARY RISK MANAGEMENT IS CONCERNED WITH:[471]

Preservation of:

- Identification
- Authenticity
- Confidentiality
- Integrity
- Non-repudiation
- Availability
- Accountability

Of information from accidental or intentional:

- Destruction
- Interference
- Use of incorrect data
- Modification
- Misrepresentation or repudiation
- Misuse or failure to use
- Access
- Disclosure or observation
- Copying or stealing
- Endangerment
- Theft
- Alteration

By

- Avoidance
- Deterrence
- Prevention
- Detection
- Mitigation
- Transference
- Sanction
- Recovery
- Correction

To

- Meet a standard of due care
- Avoid loss
- Reduce loss
- Eliminate loss
- Comply with legal regulations and statutes

[471] Represents the "New foundation of information security" as discussed by Parker "A new framework for information security to avoid information anarchy" in *Information Security – The Next Decade* (1995) 13.

STEP 3: POLICY DEVELOPMENT

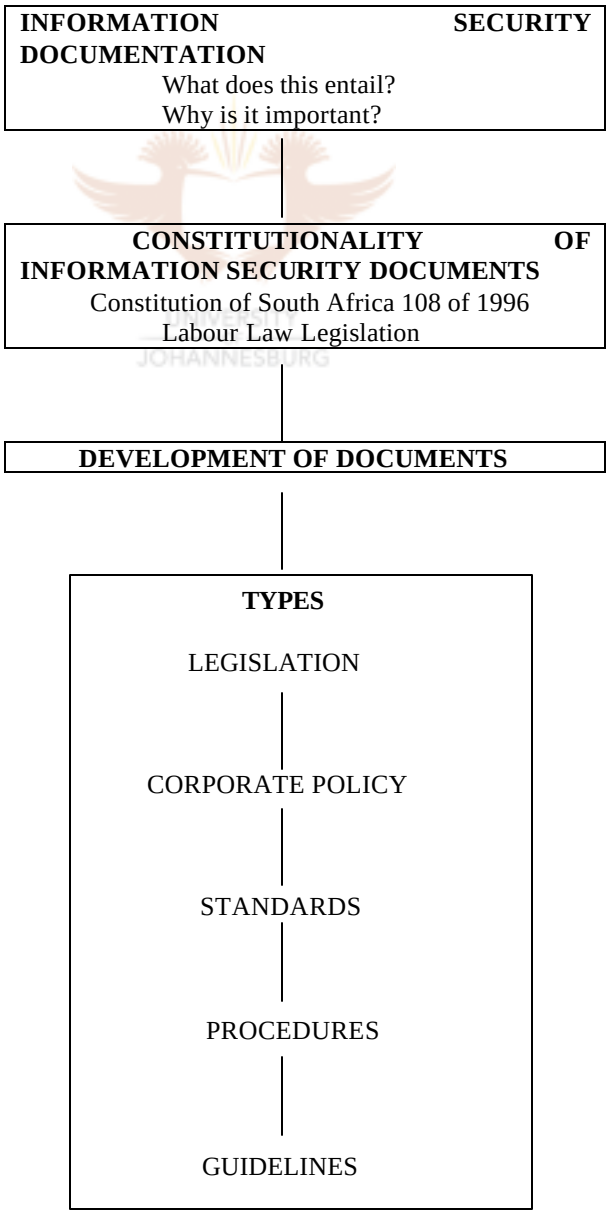
OBJECTIVE OF STEP 3:

The goal of this step is to introduce the need for adequate information security documentation within the organisation. Directors and top management must understand:

(i) What the basic types of security policies are, how they are constructed, and the hierarchical structure needed to implement and enforce these policies; and

(ii) Why the need exist to have supporting security documentation in the form of standards, procedures and guidelines.

6.3.3 ROADMAP TO INFORMATION SECURITY DOCUMENTATION



"The cornerstone of an effective information security architecture is a well written policy statement. This is the wellspring of all other directives, standards, procedures, guidelines, and other supporting documents."[472]

6.3.3.1 Information security documentation

This area is of specific importance from a legal and managerial viewpoint. The reason being that within this area the "human factor/threat" is embedded. Scheiner[473] observes that securing digital data is not the biggest problem facing organisations, but "securing the interaction between the data and the people" therein lies the problem. Research[474] have indicated that one of the biggest threats facing an organisation's information assets is the employees of the organisation themselves (the so-called internal threat).[475] The reason for this being that employees are:

(i) "behind the firewall", [476] and therefor already in the network/system of the organisation; and

(ii) they can obtain authorised access to the network through their password. [477]

Six factors which exacerbate the problems associated with the human factor/threat are:[478]

(i) How people perceive risks;

(ii) How people deal with things that happen very rarely;

(iii) The problem of users trusting computers;

---

472 Peltier *Information security Policies, Procedures, and Standards* (2002)) 21.

473 Schneier *Secrets and Lies* (2000) 255.

474 It is contended by Ernst & Young "Global information security survey 2002" (2002) http://www.ey.com/global 8 that 75% of all attacks originate from within the organisation itself, yet a survey conducted by them indicate that organisations still believe that their greatest threat will come from an external, rather than an internal source.

475 Kaleewoun "An overview of corporate computer user policy" (last visited 24 July 2002) http://www.sans.org 1.

476 ibid.

477 ibid.

478 (n 473) 256.

(iv) The futility of asking people to make intelligent security decisions;

(v) The danger of malicious insiders; and

(vi) Social engineering. [479]

To counteract this human factor/threat organisations inject information security documentation in the form of policies, standards, procedures and guidelines into the organisation. Certain legal aspects must be taken into consideration when drafting, implementing and enforcing these documents.

6.3.3.2 Constitutionality of information security documentation

> "E-commerce and related IT policies must be built on a constitutional foundation. In the light of the fact that South Africa is a developing contemporary constitutional state, one cannot develop policies in a vacuum, but must at all times consider their constitutional implications."[480]

Whenever drafting a document that might have legal implications, especially when working within the sphere of the employer-employee relationship, care must be taken not to infringe upon the employees guaranteed rights. Therefor, specific consideration must be given to rights guaranteed in the Constitution, [481] as well as in Labour Law legislation. [482]

---

[479] Social engineering has been equated to misrepresentation. Some typical examples include:
(a) The out-of-towner – A person is dressed according to office policy/environment, walking around the office shoulder surfing. It is assumed that he is from another branch or a consultant;
(b) Help-desk example - A customer phones in claiming that he has forgotten his password. He asks the employee at the help-desk to assists him in gaining access to the system. The "client" can even pretend to be a manager. The employee wanting to be helpful gives him access; and
(c) Other examples include seduction, extortion and blackmail, impersonation, flattery, sense of urgency and third-party authorisation.
Ludwig "Security awareness: preventing a lack of security consciousness" (last visited 24 July 2002) http://www.sans.org/rr/aware/lack.php 4.

[480] Jansen "IT policies must be constitutionally sound" (last visited 5 June 2002) http://www.derebus.co.za 1.

[481] 108 of 1996.

[482] (n 12) 1.

When drafting information security documentation specific consideration must be given to ensure that the following rights are not unreasonably limited or infringed upon, whether it be in a direct, or indirect manner:

A. Constitutionally guaranteed rights: [483]

(i) Section 9: The right to equality;

(ii) Section 14: The right to privacy;

(iii) Section 16: The right to freedom of expression;

(iv) Section 18: The right to freedom of association; [484]

(v) Section 23: The right to fair labour practices;

(vi) Section 32: The right of access to information; and

(vii) Section 33: The right to just administrative action.

B. Labour law rights

In South Africa labour related issues are regulated by the Labour Relations Act 66 of 1995 (henceforth LRA). Certain aspects of labour law are of specific value to the information security policy, as this is the only security document that contains a section on sanctions. Sanctions may ultimately result in the dismissal of an employee. Consequently, employers must keep the provisions of the LRA in mind when

---

[483] Keep in mind that no single right may be regarded as being absolute. All constitutionally guaranteed rights are subject to the limitation clause contained in section 36. Section 36:

(1) "The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including –
  (a) the nature of the right;
  (b) the importance of the purpose of the limitation;
  (c) the nature and extent of the limitation;
  (d) the relation between the limitation and its purpose; and
  (e) less restrictive means to achieve the purpose.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights."

[484] Chapter II of the Labour Reltions Act 66 of 1995 also protects the right to freedom of association explicitly. Some of the provisions in the LRA that inhibits the right of freedom of association inlcudes 95(5); ss 98 and 99; s 103; s 106; s 12 read with s 11; ss 25 and 26. Du Toit et al *Labour Relations Law* (2000) 84-85.

contemplating dismissing an employee for non-compliance with, for instance the information security policy, standard or procedure.

In practice, once a transgression has occurred the following procedure will be followed:

(i) "On the first occurrence the employee will be informed and given a warning of the importance to comply with the policy;
(ii) On the next occurrence the employee's supervisor will be contacted. The supervisor will discuss the indiscretion with the employee; and
(iii) Further violations of the same policy will result in disciplinary actions that might consist of suspension or possible termination, depending on the severity of the incident." [485]

A serious transgression may therefor ultimately result in a **dismissal**. [486]

It should be kept in mind that a dismissal will only be justified if the employee is guilty of serious misconduct or repeated offence. [487] Three important issues pertaining to the information security domain, are embedded in the test to be applied when determining whether or not an employee is guilty of misconduct.

(i) There must have been a **valid** or reasonable rule or standard which the employee contravened; [488]

---

[485] (n 186) 232.

[486] The LRA defines dismissal as:
(a) "Termination of a contract of employment with, or without notice [s186(a)];
(b) Failure to renew a fixed-term contract on the same or similar terms where the employee 'reasonably expected' the employer to do so [s 186(b)];
(c) Refusal to allow a female employee to resume work after: (i) taking maternity leave in terms of law, contract or collective agreement, or (ii) being absent from work for up to four weeks before the expected date of giving birth and up to eight weeks after giving birth [s 186(c)];
(d) Failure to re-employ an employee who was dismissed for the same or similar reasons as other employees, where the employer has offered to re-employ the latter ('selective non-re-employment') [s 186 (d)]; or
(e) Termination of a contract by an employee where the employer has made continued employment intolerable [s 186(e)]." Du Toit et al *Labour Relations Law* (2000) 338.

[487] Du Toit,Woolfrey, Murphy, Godfrey, Bosch and Christie *Labour Relations Law* (2000) 352.

[488] Schedule 8 item 7.

(ii) The employee must have been **aware**, or could reasonably be expected to have been aware, of the rule or standard;[489]

This section emphasises the importance of an effective information security awareness and training program which will be discussed later in this chapter.

(iii) The rule or standard must have been applied **consistently** by the employer.[490]

The enforcement of a policy in a **consistent** manner is of pivotal importance. If an employer fails to do so and allows a transgression to occur a number of times before acting against it, the employee may use the defense of legitimate expectation. Therefor the employee will state that because of the fact that he was not disciplined the previous three or four times when he committed the transgression, he had a legitimate expectation that the position would remain the same.

Furthermore, keep in mind that the two notions of unfair dismissal and unfair discrimination are very tightly bound. Consequently, a well-formulated information security policy can safeguard the organisation against lawsuits pertaining to, for instance an unfair dismissal or unfair discrimination where the employee's services was terminated because of non-compliance with the information security policy. [491]

---

489 ibid.

490 ibid.

491 When contemplating dismissing an employee the following Labour Law legislation should be consulted: Basic Conditions of Employment Act 75 of 1997, the Employment Equity Act 55 of 1998 and the Financial Skills Development Act 97 of 1998. South Africa has also incurred obligations as a member of the International Labour Organisation (ILO). The legislation and regulations that will be applicable to the organisation, will depend to a great extend on the nature of the organisation and the sector in which it functions. Du Toit (n 487) 296.

6.3.3.3 Development of information security documentation

What follows is a brief description of the standard development process followed when developing any information security document.

Phase 1: **Initiating and evaluating phase:**

A formal proposal is made to management by the security team, regarding the information security document (policy, procedure, standard or guideline), clarifying and accentuating why the need for such a document exists. [492] Thereafter management will consider the costs and benefits attached to the document. [493]

Phase 2: **Development phase**:

If management approves the document, a team[494] will be assembled to develop and research the document.[495] It is of crucial importance that the team examines existing security documentation to ensure consistency and that the same style and format is used in all relevant corporate documentation. [496]

Consensus amongst team members need to be reached regarding the proposed security document. [497] The team will advance a draft that must be presented to the "general population" of the organisation for review and comment. [498] The team must allow for a review period of at least thirty (30) days. [499] The document must also be put through a

---

[492] (n 15) 380.
[493] ibid.
[494] The composition of the team would be as follows:
- (i) Member of management;
- (ii) Members of the development team;
- (iii) Technical writer;
- (iv) Member of user community; and
- (v) Operations organisation responsible for implementation Tipton and Krause *Information Security Management Handbook* Vol 3 (2002) 380.

[495] Tipton and Krause *Information Security Management Handbook* Vol 3 (2002) 380.
[496] (n 475) 2.
[497] (n 495) 381.
[498] ibid.
[499] ibid.

series of simulations to observe its actual effect in practice. [500] After the team has taken all the criticisms, recommendations and comments into account they can finalise the document. [501] Within this phase the procurement of resources for this project will also take place. [502]

Phase 3: **Approval phase**:

During this phase the final document must be presented for approval to the appropriate organ within the organisation. [503] This duty will normally rest with the Executive Committee for Security or the governing body that performs executive level decision-making. [504]

Phase 4: Publication phase:

The final document is published within the organisation. [505] Organisations may make use of various methods to bring these documents under the attention of employees. [506] Some of these methods include a policy manual, departmental brochure or online electronic publishing. [507] Whenever choosing a method of raising awareness about the policy keep in mind that the policy will change over time and will have to be updated on a regularly basis. [508]

---

500 ibid.
501 ibid.
502 (n 495) 380.
503 (n 495) 381.
504 (n 3) 80.
505 (n 495) 382.
506 See the discussion on tools that may be used to get the security message across hereafter.
507 (n 495) 375.
508 It should be realised that the mere publication of an information security document does not guarantee or ensure that everyone, or anyone for that matter, will comply with it. The only way in which this can be ensured is through step 6 of this chapter, an information security awareness and training program. Keep in mind that awareness and training does not represent the final step. "Simply training people and making them aware (security awareness) is also not sufficient; all one gets is shallow or superficial security." Therefor employees need incentive schemes to motivate them to comply with the policy. Tipton and Krause (n 495) 229; 375.

Phase 5: Implementation phase: [509]

Even the best formulated policy is useless if it is not executed effectively. "If policies are written but never implemented, or not followed, not enforced, or enforced but inconsistently it is worse than not having them at all." [510]

The importance of **enforcement** is illustrated by Federal Sentencing Guidelines that states:

> "The standards must have been consistently enforced through appropriate disciplinary mechanisms, including as appropriate, discipline of individual responsible for the failure to detect an offence. Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific." [511]

The provisions of these guidelines are consistent with the Code of Good Practice[512] found in South African labour law which states that when determining if an employee may be dismissed on the ground of misconduct or non-compliance, one of the factors that must be taken into consideration is whether or not "the rule or standard has been consistently applied by the employer."[513]

> "Strict enforcement of policy and standards must become a way of life in business. Corporate policy making should consider adherence to them a condition of employment. Never adopt a policy unless there is a good prospect that it will be followed. Make protecting the confidentiality, integrity and availability of information 'the law'." [514]

---

509 (n 495) 382.
510 (n 186) 228.
511 ibid.
512 This code is found in Schedule 8 of the Labour Relations Act 66 of 1995.
513 Code of Good Practice Schedule 8 item 7.
514 (n 186) 229.

Phase 6: Review the document on a regular basis taking into account the policy, posture and practice. [515] It is recommended that policies should be reviewed at minimum on an annual basis. [516] Furthermore, keep in mind that just as employees sign the original information security policy they must also sign subsequent revisions.[517]

6.3.3.4 Information security documentation hierarchy

The discussion which follows is based on the following hierarchy:

[515] "…check security posture to ensure that the defense in depth methodology you have employed is secure; the practice is about keeping your users informed of the policies and best security practices that they can do their part in security...". Dulany "Security, it's not just technical" (last visited 25 July 2002) http://www.sans.org 4.

[516] Dulany "Security, it's not just technical" (last visited 24 July 2002) http://www.sans.org 4.

[517] Lindley "Technical writing for IT security policies in five easy steps" (last visited 24 July 2002) http://www.sans.org 6.

Legislation

("Legislation is established by government, which in turn often creates policy that may or may not be enacted in legislation"). [518]

Corporate Policy

("States goal in general terms"). [519]

Standard

("Define what is to be accomplished in specific terms").[520]

Procedure

("Step-by-step reference guide telling employees how to meet the standards").[521]

Guidelines

(They are general recommendations of what organisations would like to see its employees do").[522]

[518] Legislation will have an impact on the organisation regardless of its size Tipton and Krause (n 495) 365.
[519] (n 51) 70.
[520] ibid.
[521] (495) 365.
[522] (n 495) 365-366.

6.3.3.5 Information security policy [523]

(i) The information security policy in context

(a) Defining the information security policy

Numerous definitions have been advanced for the term "policy".[524] The researcher favors the following definition. Policies in general may be defined as a document:

> "designed to inform all individuals operating within an organisation of how they should behave related to a specific topic, how the executive management of the organisation feels about the topic, and what specific actions the organisation is prepared to take related to that topic."[525]

A policy "is a high level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specific subject area."[526]

Elaborating on the general definition advanced for a policy,[527] an information security policy may be enumerated as follows:

> "A security policy establishes what must be done to protect information stored on computers. A well-written policy contains sufficient definition of "what" to do so that the "how" can be identified and measured or evaluated. An effective security policy also protects people. Anyone who makes decisions or takes action in a situation where information is a risk incurs personal risk as well. A security policy allows people to take necessary action without fear of reprisal. Security policy compels the safeguarding of information, while it eliminates, or at least reduces, personal liability for employees."[528]

---

523 See Annexure L for an example of an information security policy.

524 Tipton and Krause (n 495) 353 define a policy as: "…a set of practices that regulate how the organisation manages, protects, and assigns resources to achieve its security objectives…".

525 (n 3) 79.

526 (n 472) 21.

527 Mistry "Developing security policies for protecting corporate assets" (last visited 24 July 2002) http://www.sans.org 1 defines an information security policy as: "(s)ecurity policies govern the steps and procedures taken to protect business assets and confidential information from intrusion via the use of technology or physical intervention."

528 (n 15) 1.

This excerpt accentuates why the need for information security policies exist, namely to reduce, and **f** possible eliminate personal liability of employees, and as will later be indicated, that of directors as well.

(b) Characteristics of a policy include:

(i) Short, enforceable, and changes infrequently; [529]

(ii) Set at a high level and approved by management; [530]

(iii) Few policies exist within the organisation; [531] and

(iv) Refrain from containing a detailed description of how to implement the policy. [532]

(c) Objectives of an information security policy

An information security policy has main objectives which exist in an internally and externally domain. Internally the policy will depict what is required of the employees of the organisation, and what consequences will ensue if they do not adhere to the policy. [533] Externally it gives the "world" insight into how the organisation operates and functions. It will further provide reassurance to stakeholders that the organisation is taking appropriate steps to safeguard its information assets. [534]

529 (n 186) 235.
530 (n 472) 25.
531 ibid.
532 ibid.
533 (n 472) 21.
534 ibid.

(d) Demand for information security policies

The question may be asked why the need for an information security policy exist within an organisation?

In general organisations are motivated to implement information security policies by five major consequences that may ensue if they do not have this policy in place:

(i) Loss of competitive advantage;[535]

(ii) Loss of customer and shareholder confidence;[536]

(iii) Increased governmental interference;[537]

(iv) Non-compliance with legislative requirements;[538]

Certain legal requirements demand that policies and procedures are in place. Amongst these requirements we encounter the duty care and skill/due diligence. [539]

The importance of security documentation lie in the fact that they will have an impact should there be an incident that calls the operation into question. This statement may be corroborated by a practical example found in the United States of America:

> "There are federal sentencing guidelines for criminal conviction at the senior executive level, where the sentence can be reduced if there are policies and procedures that demonstrate due diligence. Effectively this means that having an effective compliance program in place to ensure that the corporation's policies, standards are in

[535] McLeod and Schell (n 210) 28 define a competitive advantage as: "…the use of information to gain leverage in the marketplace…".
[536] (n 472) 23.
[537] ibid.
[538] (n 495) 359.
[539] The duties that directors are placed under in terms of the common law will be discussed in greater detail in chapter seven below.

place can have a positive effect in the event of a criminal investigation."[540]

(v) Risk of legal liability increases.

Even if an organisation is not legally bound to develop and implement an information security policy, such a policy will proof to be beneficial to the organisation for the following reasons:

(a) As stated earlier information security is concerned with the protection of its 5 pillars. It therefor stands to reason that information security policies will strive to find a way to best conduct business while simultaneously protecting the identity, authenticity, confidentiality, integrity,[541] and non-repudiation of the information assets of the organisation;[542] and

(b) The possibility of litigation is reduced over issues pertaining to wrongful termination; discrimination; unfair labour practices and theft.[543]

Voges[544] observes that "Internet law is still very confusing, but enterprises with [information security] policies in place can protect themselves from unnecessary headaches." He goes on to observe that companies who have an effective information security policy that recognises and complies with internationally acceptable standards,

---

540 (n 495) 360.

541 Hare is of the opinion that security policies will mainly focus on the first two attributes, namely confidentiality and integrity. It is interesting to observe that these two attributes of information "…are normally in conflict with one another, because of their different objectives…" Confidentiality is concerned with "…the privacy of, and access to information…" whereas integrity is concerned with "…preventing the modification of information ensuring that it arrives correctly when the recipient asks for it…". This conflict can clearly be illustrated by investigating the strain existing between the Bell and Lapadula model (confidentiality-based) and the Biba and Clark-Wilson model (integrity based). These three models represent the three formal security models. "A security model defines a method for implementing policy and technology" Tipton and Krause (n 495) 354-358.

542 Mistry "Developing security policies for protecting corporate assets" (last visited 24 July 2002) http://www.sans.org 1.

543 Voges "IT needs security partnership with HR" (last visited 20 February 2002) http://www.computingsa.co.za 2.

544 ibid.

will have a distinct advantage over those companies who adopt a "wait-and-see" attitude.[545] Companies who do not have an information security policy in place, or do have such a policy, but the policy is not effectively enforced, are earmarked as being prone to fall victim to attacks from hackers and crackers and other threat agents.[546] This will ultimately result in loss of customer confidence and shareholder value.[547]

After reviewing why the need for information security policies exist, it should be clear that organisations (and specifically the board of directors) may be labeled as being reckless, negligent and irresponsible if they allow the organisation to function without having an effective information security policy in place. In practice however, we still encounter numerous organisations that are willing to take this risk, be it out of arrogance or mere ignorance.

The researcher will therefor briefly focus on the situation where **organisations attempt to function with an unwritten information security policy.**

It is common practice for organisations to function without a formally written information security policy. [548] The unwritten information security policy is much like a custom[549] passed on by one employee to the other by word of mouth. [550] However, this results in uncertainty, confusion and possible grounds for legal action. One of the most prevalent problems experienced in this regard is that no roles or responsibilities have been formally assigned to employees. Therefor problems will arise when top management wants the hold an employee liable for non-compliance. These problems include: (i) no explicit role or responsibility has been assigned to the employee, and/or (ii) if such a role or responsibility has been assigned, the employee is unaware of this role

---

545 ibid.
546 ibid.
547 ibid.
548 (n 472) 23.
549 Within a legal context a custom may be defined as: "…a fixed practice in accordance with which people live because they regard it as law…". Four requirements must be met before a custom will qualify as law: (i) a custom must have existed over a long period; (ii) it must be observed by the community in which it applies; (iii) it must be reasonable; and (iv) its content and meaning must be certain and clear. Visser and Potgieter *Introduction to Family Law* (1998) 12.
550 (n 472) 23.

or responsibility.[551] The doctrine of legitimate expectation[552] may again here be utilised by the employee.

Unwritten policies, procedures and standards may open the organisation up to potential liability. The following citation from Tudor[553] highlights the inherent dangers prevalent in not having a formal written information security policy:

> "…it is very difficult to test for the effectiveness or compliance anything that is undocumented. In addition, it has been set as a legal precedence that companies must show or prove due care when enforcing policies, in which case they have made an effort to be in compliance, in a minimum, with industry standards. From a legal perspective enterprises must be prepared to show that they have communicated to their employees, users of their system, and business partners, appropriate use of those systems and resources as well as appropriate ways to effectively protect their business, information, and resources, from damage, theft, destruction, or unauthorized access. This will minimize the risk of legal liability due to negligence and breach of fiduciary responsibility."

Ultimately the question must be asked why organisations would willingly open themselves up to potential legal liability in such a reckless manner if the implementation of an austere policy could protect them? It should be evident from the preceding discussion that the primary reason for having an information security policy is to aid directors and top management alike in having concrete evidence to present to a court of law, customer contract, a vendor relation, acquisition, or for public relations, as proof of fulfillment of their responsibility of due diligence. [554]

---

551 ibid.

552 Neither the interim constitution, nor the 1996 Constitution advanced a definition for the concept of legitimate expectation. The courts have however taken it upon themselves to develop tests and guidelines concerning this principle. In one of South Africa's leading cases on this subject matter *Administrator, Transvaal, & others v Traub* 1989 (4) SA 731 (A), the court remarked that "…legitimate expectations' are capable of including expectations which go beyond enforceable legal rights, provided they have some reasonable basis..." (756G-H). The court went further to state "(l)egitimate, or reasonable, expectation may arise either from an express promise given on behalf of a public authority or from the existence of a regular practice which the claimant can reasonably expect to continue…"(756I). For a comprehensive discussion on what this concept entails, as well as an historical overview of how it was introduced into the South African legal system, consult the Traub-case. Within the ambit of the information security policy the employer might argue that he had a legitimate expectation that the employee would comply with the policy/standard/procedure. The chances of the employer being successful with this argument is however uncertain.

553 (n 3) 80.

554 (n 472) 23.

Apart from the multitude of legal and regulatory reasons advanced to indicate the benefits attached to having an information security policy, the implementation of such a policy will result in better control over the organisation which ultimately makes good business sense. [555] It is required of top management to exercise control over the organisation otherwise the organisation and/or the board of directors in their personal capacity, might face financial penalties in the form of fines and costs. [556]

(ii) Information security policy development

The responsibility for the development and implementation of the information security policy rests with the security team. Because of this the composition of the security team is of pivotal importance. In the past it was common practice for management to assign the task of development and implementation solely to IT security professionals. This resulted in policies not reflecting legal and/or business aspects and concerns of the organisation. [557] Furthermore these professionals often lacked the necessary writing skills to create "readable, concise and effective written communication". [558]

(a) Policy manuals

It is expected of organisations to have at least two policy manuals in place to address the 2 broad issues of:

(i) The use of the website; and

(ii) The use of communication systems by employees. [559]

---

555 (n 472) 24.
556 ibid.
557 (n 517) 1.
558 ibid.
559 De Villiers "Website and e-mail policies" (August 2003) *E-Commerce Law 3* 1.

These two issues can effectively be covered in two umbrella policy manuals, namely

(i) Website use policy; and

(ii) Communications systems policy. [560]

(i) The **website use policy** will regulate the use of the organisation's website.[561] Therefore, this policy will stipulate how a webiste user may use the website. This policy will address issues such as:

(a) Who may use the website; [562]

(b) How must the website be used; [563]

(c) The liabilities of the website owners; [564]

(d) The protection of the intellectual property rights of the websites; and [565]

(e) How disputes will be resolved. [566]

For purposes of this discussion, the second umbrella policy is of particular importance, as the information security policy will fall within the scope of this policy.

(ii) Communication systems policy

This policy may be viewed as a general policy that dictates the overall use of communication systems[567] within the organisation. [568] The communication system policy may be viewed as the title of a manual that will contain other policies.

---

560 ibid.
561 (n 559) 9.
562 (n 559) 10.
563 ibid.
564 (n 559) 13.
565 (n 559) 14.
566 (n 559) 20-21.
567 Within this context a communication system will include, but is not limited to: (i) telephones; (ii) cellular phones; (iii) fax machines; (iv) e-mail; and (v) the Internet.
568 (n 559) 2.

At minimum this policy/manual will include:

(i) "a clear description of appropriate and inappropriate use for both business and private communications;
(ii) provisions relating to security of communication systems; and
(iii) provisions dealing with monitoring of communications."[569]

This policy will be applicable to all employees, regardless of their position or level of employment within the organisation.[570]

This manual will result in subsequent policies being developed and implemented in the following areas:

(a) Acceptable Internet usage policy;[571]
(b) **Information security;**[572]
(c) E-mail policy;[573]
(d) Back-up and recovery policies (Disaster recovery);[574]
(e) Remote access policy;[575]
(f) Contingency planning policy;[576]
(g) Virus protection policy;[577]
(h) Encryption policy;[578]

569 (n 559) 3.
570 (n 559) 2.
571 In Australia companies are required by law to have in place a security policy as well as an Acceptable Internet Usage Policy. South Africa is however lagging far behind when it comes to security legislation. Middleton "SA lags electronic security legislation" (last visited 24 July 2002) http://www.itweb.co.za 1.
572 (n 495) 369.
573 E-mails can pose numerous threats including, but not limited to unsolicited e-mails; e-mail attachments that are not scanned for viruses before being opened; inappropriate e-mails that may expose the organisation to litigation pertaining to sexual harassment, discrimination or hate speech. Symantec "Internet abuse – the enemy within?" (last visited 18 April 2002) http://www.itweb.co.za 2. For more information on e-mail policies, consult Tudor (n 3) 85-88.
574 The future existence of an organisation may depend on the quality of its back-up and recovery systems. This policy is the safety net that assures management that if something does go wrong the organisation will be able to recover.
575 (n 516) 7.
576 ibid.
577 ibid.
578 ibid.

(i) Incident response policy;[579]

(j) Wireless/PDAs policies;[580] and

(k) Password policy.[581]

(b) Initial information security policy assessment

Two situations should be distinguished under this heading:

(i) Where the organisation does not have any information security policy in place;[582] and

(ii) Where the organisation does have an existing information security policy in place. [583]

In case of the former situation, an investigation must be launched into the strategy of the organisation, as well as analyzing any existing policies of the organisation. The reason for this being that there must be consistency in the format and style of all organisational documentation. [584]

---

579 ibid.

580 ibid.

581 Password should not be equated to privacy. A password merely allows authorised users access to information. There are three rules whenever using passwords within the organisation:

(i) Use frequently;
(ii) Change often; and
(iii) Do not share with anyone.

Password should not be any of the following:

(i) Dictionary words;
(ii) Anyone's or anything's name;
(iii) A place;
(iv) A proper noun;
(v) A phone number;
(vi) Password of the same character;
(vii) Simple patter of letters on keyboards;
(viii) Any of the above reversed or concatenated; or
(ix) Any of the above with digits appended. Von Solms, Eloff J, Eloff M and Smith *Information Security* (2001) 24-27.

582 Unknown "Policy framework for interpreting risk in e-commerce security" (last visited 2 November 2002) http://www.cerias.purdue.edu/techreports-ssl/public/pfires 11.

583 ibid.

584 ibid.

(c) Writing of the policy

When writing the information security policy the security team must consider five basic questions:

(i) What is the intent of the policy?
(ii) Who is affected? (roles and responsibilities?)
(iii) Where does the policy apply? (scope?)
(iv) When does the policy take effect? "[585] and
(v) Why is it necessary to implement the policy?[586]

A standard format for information security policies

It is important to establish a definite style/format in which all policies, standards, procedures and guidelines will be written. This will ensure consistency and will effectively rule out the possibility of confusion. [587] Although it is acknowledged that each organisation will design and write their procedures, policies, standards and guidelines in a manner that is pertinent to that specific organisation, the following configuration is considered to be the established format for all major headings and topics within information security policy documents: [588]

(i) **Background** why the policy exists: the importance of security as an enabling mechanism for information sharing;[589]
(ii) **Scope:** who the policy affects and where the policy is required;
(iii) **Definitions:** explanation of terminology;[590]

[585] (n 495) 371-372.
[586] ibid.
[587] (n 495) 376.
[588] (n 495) 375.
[589] (n 472) 31-32.
[590] ibid.

(iv) **References** where people can look for additional information, eg. more detailed security policies and procedures;[591]

(v) **Coordinator/policy author:** who sponsored the policy, and where do people go to ask questions?

(vi) **Authorising officer:** who authorised the policy?

(vii) **Effective date:** when the policy takes effect;

(viii) **Review date:** when the policy gets reviewed;

(ix) **Disposal:** Details pertaining to the disposal of sensitive information;

(x) **Policy statement:** what must be done;

(xi) **Exceptions:** how exceptions are handled; and

(xii) **Sanctions:** what actions are available to management when a violation is detected. [592]

It is important to bear in mind that the question of "how" the policy will be implemented or complied with should not be addressed in the policy document, "too often policy writers include how things should be done, however good policies generally establish only what must be done and why it must be done, but not how to do it."[593]

(iii) Information security acknowledgement form [594]

From a legal perspective two important aspects still need to be addressed concerning information security policies: firstly, how to ensure that employees are legally bound to the information security policy, standard, or procedure; and secondly, how to make employees aware of the information security policies, standard, procedure and guidelines.

---

591 ibid.
592 (n 495) 372.
593 (n 517) 1.
594 In the United States of America the information security acknowledgement form is used effectively in practice Tudor (n 3) 82. See Annexure M for an example of an information security acknowledgement form.

It is generally required of all newly appointed employees to sign a service contract in which the information security policy will be incorporated. The problem however arises when the organisation has existing employees that did not sign the policy when they were first appointed. The reason for this being that, for instance such a policy did not exist at the time of their appointment. An effective solution to this problem would be to require of existing employees to sign an information security acknowledgement form before he/she receives any future/further computing assets. By adopting the terms "computing assets" the organisation does not limit itself to specific applications or programs. Consequently, it may be required of an employee to sign the acknowledgement form regardless whether he is receiving a new laptop, desktop, software or hardware. It may even be something as small as a network cord.

The **implementation of the acknowledgement form** would entail he following:

(i) "A digested version of the [information security] policy can be developed into a Security Policy Acknowledgement Form";[595]

(ii) New employees are required to read and sign this form upon employment at the organisation and prior to receiving computing assets;[596]

(iii) It is required of existing employees to read and sign this form prior to receiving any new or further computing assets;[597]

(iv) It is desirable that the acknowledgement form is signed on a periodical basis to remind the employees of their responsibilities to protect the confidentiality, integrity and availability of the information and processing resources;[598] and

---

595 (n 3) 82.
596 ibid.
597 ibid.
598 ibid.

(v) "The signature can be used to validate that the user has been informed and understands his/her responsibilities."[599]

Content of this form:

(i) Defines what the user is to protect; [600]

(ii) Scope of resources; [601]

(iii) What his/her responsibility is to protect the resources;[602] and

(iv) Acknowledgement statement of the user's understanding. [603]

It is very important that the information security acknowledgement form is reviewed by both the human resource and the legal department of the organisation in order to ensure that it is in line with existing corporate policies, and will be considered legally binding by a court of law. [604]

After the information security policy has been developed and implemented a security and control framework needs to be developed consisting of standards, procedures and guidelines that will reinforce and support the information security policy.

599 (n 3) 84.
600 ibid.
601 ibid.
602 ibid.
603 ibid.
604 ibid.

6.3.3.6 Information security standards [605]

(i) Defining standards

Standards may be defined[606] as "mandatory activities, actions, rules, or regulations designed to provide policies with the support structure, and specific direction they require to be meaningful and effective."[607]

(ii) Characteristics of a standard include:

(i) A standard is derived from a policy; [608]

(ii) It is more flexible than policies, and can adapt with greater ease to changing circumstances; [609]

(iii) It is generally tied to a subject; [610]

(iv) A standard must support the mission statement;[611]

---

[605] There are certain groups created with the sole purpose of developing standards. Amongst these groups we find:

(i) ANSI: the American National Standards Institute;
(ii) ECMA: European Computer Manufacturers Association;
(iii) EDPAA: Electronic Data Processing Auditors Association;
(iv) EIA: Electronic Industries Association;
(v) IAB: Internet Architecture Board;
(vi) IESG: Internet Engineering Steering Group;
(vii) ISO: International Standards Organisation;
(viii) NIST: National Institute of Standards and Technology; and
(ix) NAS: National Security Agency Tudor (n 3) 93.

Unfortunately no single, universal applicable information security standard exists. This results in "standard shopping" with organisations selecting standards that will best support their ulterior motives. The development, implementation and enforceability of a universal standard is however feasible as is evident from Generally Acceptable System Security Practices (GASSP). Herold (ed) *The Privacy Papers* (2002) 216.

[606] Tudor (n 3) 79 defines standards as: "…a specific set of rules, procedures or conventions that are agreed upon between parties in order to operate more uniformly and effectively…standards set a level of expectation that must be reached or exceeded in order to fulfill one's obligations or responsibilities…".

[607] (n 472) 26.

[608] (n 495) 365.

[609] ibid.

[610] (n 472) 71.

[611] A mission statement may be composed of "…a brief paragraph explaining the overall goals of the information security program. Expands what was said in policy statement into goals to be addressed by your department…" Peltier (n 472) 56.

(v) "It defines specific, measurable statements that can be used to subsequently verify compliance"; [612] and

(vi) Standards must be reasonable, flexible and current.

Some of the most important information security standards that organisations will have to consider include:

(i) ISO[613] 17799; [614]

(ii) Control Objectives for Information and Related Technology (henceforth COBIT);[615] and

---

612 (n 495) 365.

613 The International Organisation for Standardisation was founded in 1947. "It is a worldwide federation of national standards bodies from approximately 100 countries, one from each country. ISO is not an abbreviation. It is a word, derived from the Greek *isos*, meaning equal, which is the root for the prefix ïso-that occurs in a host of terms, such as isometric (of equal measure or dimension) and isonomy (equality of laws, or people before the law). The name ISO is used around the world to denote the organisation, thus avoiding the assortment of abbreviations that would result from the translation of International Organisation for Standardisation into different national languages of members. Whatever the country, the short form for the organisation's name is always ISO" Roberts (n 4) 23.

614 ISO 17799 is a standard for information security has been widely recognised and adopted. The following reasons may be advanced why the standard has gained wide-spread support and acceptance:

(a) The increased use of e-commerce has highlighted the importance of trust and security. Organisations themselves, as well as their customers want to be reassured that they are conducting business in a relatively safe environment;

(b) At present major consultancy firms employ this standard;

(c) This standard improves quality;

(d) The pressing issues which existed at the time of BS 7799's inception plays a much more subordinate role now (eg Y2K, EMU); and

(e) Organisations are beginning to realise that ISO 17799 will give "first adopters" a competitive advantage – "what if competitors are more advanced than you, consider what will happen if they become certified. They may then join the others in making certification a market differentiator. Obvious scenario, for instance a corporate customer choosing between two similar services for which security is a concern. Will depend if they are ISO security certified."

Unknown "The ISO directory" (last visited 14 July 2003) http://www.iso-17799.com 7-8. Although corporate South Africa does not legally require of companies to comply with this standard, and no such a legal requirement can be envisioned in the near future, top management will do well to take note of, and adhere to this standard. In 2002 13% of corporate South Africa have implemented ISO 17799, and another 15% were planning to in 2003. KPMG "The ultimate security is your understanding of reality" (last visited 5 June 2002) http://www.itweb.co.za 2.

Benefits attached to compliance with ISO 17799 include:

(i) This standard represents a good information security practice;

(ii) It ensures better risk management;

ISO 17799 will help build consumers and shareholders confidence in the organisation. For an overview of the key issues ISO 17799 address see Annexure A.

615 See Annexure A for a comprehensive outline of this information security standard.

(iii) OECD Guidelines for Information Security Systems and Networks.[616]

6.3.3.7 Information security procedures

(i) Defining procedures

Procedure are defined[617] as:

> "plans, processes, or operations that address the specifics of how to go about a particular action. They enable the transfer of knowledge between individuals who perform the same job, cover for each other during absence, or allow for more knowledgeable transition during permanent changes of staff."[618]

Procedures typically answer the more guided questions of "where, when and how", while policy answer "who, what and why".

(ii) Characteristics of procedures:

(a) Procedures are not written by the security team. The input of employees who deal with the day-to-day functioning of the operation will have to be obtained;[619]

(b) Procedures are recommendations;[620]

(c) Procedures must be written in a great amount of detail; [621]

---

616 See Annexure A for a comprehensive outline of this information security standard.

617 Peltier (n 472) 26 defines procedures as: "(p)rocedures spell out the specifics of how the policy and supporting standards and guidelines will actually be implemented in an operating environment."; Tudor (n 3) 96 defines procedures as: "(p)rocedures should reflect best practice or, through the repetitive nature of performing a specific task, improvements that have been made to the process to provide for efficiency."

618 (n 3) 80.

619 (n 3) 97.

620 (n 472) 83.

621 The writing of the procedure might represent difficulties due to the amount of detailed required Tipton and Krause (n 495) 373.

(d) Procedures are flexible enough to adapt to changes occurring within the business and technological environment; [622] and

(e) "Procedures are as unique as the organisation itself."[623]

(iii) Objectives of a procedure

Peltier[624] identifies the following objectives of a procedure:

(a) "Fulfill some need;

(b) Identify target audience;

(c) Describe the task that the procedure will cover; and

(d) The intent of the procedure should also be made known to the user."

6.3.3.8 Information security guidelines

(i) Defining guidelines

Guidelines may be defined as being "more general statements that are designed to achieve the objective of the policy by providing a framework within which to implement procedures." [625]

The most important **characteristic of a guideline** is that compliance with the guideline is optional. [626] It is therefor the employee's own decision if he/she wants to comply with the guidelines. [627]

---

622 (n 472) 25.
623 (n 495) 373.
624 (n 472) 86.
625 (n 495) 375.
626 ibid.
627 ibid.

OUTCOMES DELIVERED BY STEP 3:

(i) Information security documents will provide the foundation on which any information security governance initiative must be build; [628] and

(ii) Information security documentation provide directors and top management with a mechanism to enforcement information security within the organisation, as employees may be held accountable for non-compliance with such a document.

[628] (n 186) 221.

STEP 4: ASSIGN ROLES AND RESPONSIBILITIES

OBJECTIVES OF STEP 4:

Roles and responsibilities must be assigned for the implementation of information security governance within the organisation, thereby enabling:

(i) The employees to have certainty regarding their function, responsibilities and obligations within the implementation process; and

(ii) The organisation to hold an employee accountable for failure to perform his duties.

"To protect the confidentiality, integrity and availability of information, organisations must ensure that all individuals involved understand their responsibilities." [629] This objective is achieved through:

(i) The information security policy in which responsibilities are assigned to designated employees or groups of employees; [630] and

(ii) An awareness and training program in which the aforementioned employees are made aware of, and educated on their responsibilities. [631]

Therefor, the assignment of roles and responsibilities will flow from the information security policy, standard, procedure and guideline.

OUTCOME DELIVERED BY STEP 4: each employee knows exactly what is expected of him, and what they can be held accountable for.

---

629 (n 495) 318.

630 Organisation for Economic Co-operative and Development "OECD guidelines for the security of information systems and networks" (last visited 10 September 2003) http://oecd.org 10.

631 Tozer "Leadership skills" in Aalders and Hind *The IT Manager's Survival Guide* (2002) 226.

STEP 5: ALLOCATION OF ADEQUATE RESOURCES TO INFORMATION SECURITY EFFORTS

OBJECTIVES OF STEP 5:

Enabling directors and top management alike to make informed decisions regarding resource allocation for information security efforts.

The allocation and demand for resources will inevitably depend on the level of information security required within the organisation.[632] Furthermore the degree to which the board is willing to make resources available will reflect their commitment to information security efforts.[633]

[632] Cazemier, Overbeek and Peters *Best Practice for Security Management* (2002) 16.

[633] Examples of resources include time, skilled personnel and finances. The most conspicuous resource would be financial resources – the budget.
How does an organisation go about establishing a budget? One of three approaches may be followed:

(i) The top-down approach:
The executive determines the budget and then enforces it on the lower levels of the organisation. Reasoning behind this process is that executives have an overall picture of what the organisation wants to achieve and how to do it. Critisism that may be launched against this approach is that executives are detached from the day-to-day running of the company and this may result in an exorbitant budget;

(ii) The bottom-up approach:
According to this approach, employees on the lower levels of the organisation ascertain the budget and this is communicated to upper levels of the organisation. An advantage of this approach is that the people who are involved in the day-to-day activities of the organisation determine the budget. Top management may however argue that, because of the fact that lower-level employees do not have a comprehensive view of the organisation, they set unrealistic targets; and

(iii) The participative approach:
Because of the criticism launched against both of the previous approaches a compromise was reached in the form of the participative approach. This approach allows for the participation and consultation of managers from various levels within the organisation to reach a concession that is acceptable to all. At present this process is gaining widespread acceptance Cazemier (632) 16.

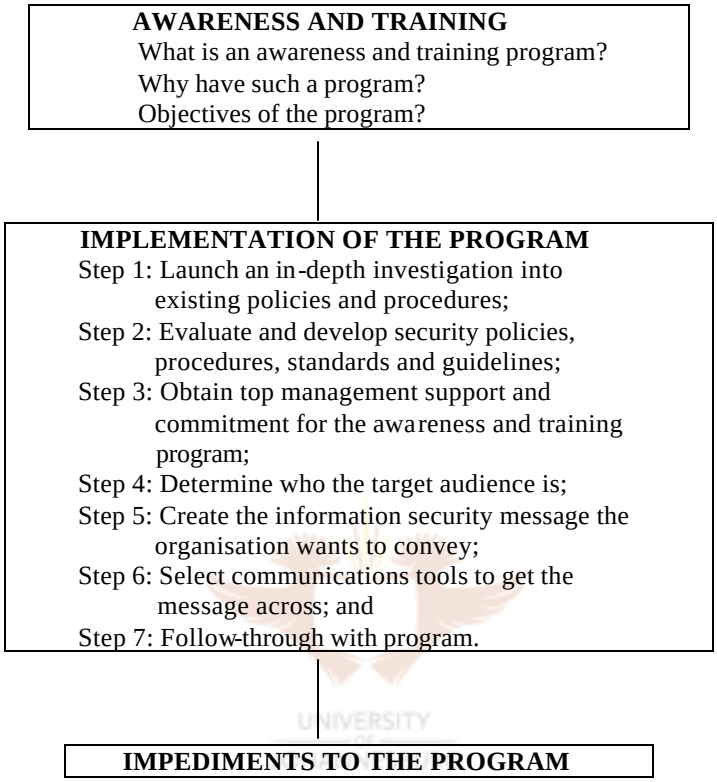
It is recommended that organisations, whenever possible, have a definite budget for information security.[634] This will accommodate planning and the setting of goals for information security initiatives and programmes.

OUTCOME DELIVERED BY STEP 5: the importance of information security within an organisation is realised and acknowledge, and this results in adequate resources being allocated to information security efforts.

[634] A recent survey conducted by KPMG indicated that corporate South Africa spend 1% to 10% of their IT budget on information security. This is despite the well-known fact that it is much more cost-effective to invest in security up-front, than to try and recover afterwards. KPMG "The ultimate security is your understanding of reality" (last visited 5 June 2002) http://www.itweb.co.za 2.

STEP 6: AWARENESS AND TRAINING

ROADMAP TO INFORMATION SECURITY AWARENESS AND TRAINING



OBJECTIVE OF STEP 6:

(i) The main objective of this step is to make employees on all levels of the organisation aware of information security practices, procedures and documentation.

6.3.6.1 Information security awareness and training in context

The essence of an information security awareness and training program is best captured by the following quotation: "…if the road to hell is indeed paved with good intentions, then the sidewalks are built of grand ideas that never saw the light of day or languished as the best kept secret within the corporate walls".[635]

Although the development and implementation of information security policies, standards, procedures and guidelines are imperative to the success of the overall information security governance discipline, it will be a futile exercise if these policies, guidelines and procedures are not brought under the attention of those people who are expected to adhere to them, therefor the employees of the organisation.[636] The importance of awareness and training can not be overemphasised as observed by Tipton and Krause[637] "an effective security awareness program could be the most cost-effective action management can take to protect its critical information assets." Employees are often viewed as the first line of defense when it comes to the early detection of problems.[638]

Consequently, employees on all levels of the organisation must be made aware of the pivotal role security, and specifically information security plays within an organisation.[639] They need to be educated on, and kept informed of potential threats, vulnerabilities and risks, and shown how their actions could increase or decrease the likelihood of a threat materialising.[640] "All employees must be sensitive to security."[641]

(i) Defining awareness and training

---

635 Desman *Building an Information Security Awareness Program* (2002) 101.
636 (n 48) 197.
637 ibid.
638 (n 631) 10.
639 (n 632) 80.
640 (n 631) 10.
641 Atkins "Jesse James at the terminal" (July-August 1985) *Harvard Business Review* 84.

Although the terms awareness and training are often used concurrently, they are not synonymous with one another. A clear distinction should therefor be drawn between awareness and training. Awareness is "a passive mechanism that occurs through less formal methods such as posters, themes and objects such as key rings and cups."[642] It is contended by Russel[643] that the goal of awareness is "to raise the collective awareness of the importance of security and security controls."

Training or instructional design, may be viewed as being "more formalised, typically in a classroom, or conference setting where the objective is to gain knowledge about a particular subject."[644] Russel[645] argues that the goal of training is "to facilitate a more in-depth level of user understanding."

For the purpose of this research paper information security awareness and training may be defined as the process by which all role players in the organisation are made aware of what the information security policies, standards, procedures and guidelines entail, what is expected of them, why this is expected of them, and what consequences would ensue if they do not adhere to/comply with these policies, standards, procedures and guidelines.[646]

(ii) Awareness and training program objectives

The first and foremost **objective** of any information security awareness and training program is to give prominence to the importance of information security within the organisation, and raise the consciousness of all employees regarding this subject-matter.[647]

---

642 (n 3) 147.
643 Russell "Security awareness – implementing an effective strategy" (last visited 31 March 2003) http:// www.sans. org/rr/aware.php 3.
644 (n 3) 147.
645 (n 643) 3.
646 Memory "Security awareness – everybody's business" (last visited 31 March 2003) http://www.sans. org/rr/start/ everyone.php 1.
647 (n 635) 319.

Other objectives include:

(a) Enabling employees to recognise their responsibility for protecting the organisation's information assets [648]

Employees must realise that information security forms part of their job.[649] By tying information security responsibilities to their job description employees can understand the importance of information security and the concept of ownership for it.[650] It must be made clear to employees that information security is everybody's responsibility,[651] it forms part of the corporate culture.[652]

(b) Ensuring that employees realise the value of information security [653]

The program must be developed in such a way that it "defines exactly how corporate information assets are defined, who uses them, and what steps must be taken to protect them."[654] Employees must be made aware of the value of the organisation's information assets by emphasising the legal and financial consequences that will ensue if the confidentiality, integrity and/or availability (CIA) of information assets are not adequately protected.[655]

(c) Enabling employees to recognise potential violations and know who to contact [656]

---

[648] (n 3) 139.
[649] ibid.
[650] (n 3) 140.
[651] ibid.
[652] Corporate culture may be defined as the beliefs and values shared by people in an organisation, and is akin to the personality of the organisation. It comprises of an omnipresent set of assumptions that is often difficult to fathom and that directs activities within the organisation.
[653] (n 3) 140.
[654] (n 635) xvi.
[655] (n 3) 140.
[656] (n 3) 142.

Apart from making employees vigilant by highlighting what risk and threats must be guarded against, they should also be informed of the correct procedure to be followed from the moment a security incident or potential security incident has occurred.[657] Warning signs and indicators must furthermore be implemented and pointed out to employees on when a potential threat arises.[658]

(d) "Ensuring that the level of security awareness and training among existing employees remains high."[659]

Training should be offered to new recruits, as well as to existing employees.[660] All employees need to be kept up-to-date on the latest development on new and existing threats, vulnerabilities and risks facing the organisation.

6.3.6.2 Implementing the awareness and training program

The following framework will assist organisations in developing and implementing the information security awareness and training program.

Keep in mind that the development and implementation of the information security awareness and training program is a managerial issue, therefor the chief information officer will typically be responsible for the development, implementation and maintenance of the program. [661]

Step 1: Launch an in-depth investigation into policies and procedures that already exist

---

657 ibid.
658 ibid.
659 (n 3) 146.
660 (n 3) 147.
661 (n 632) 80.

within the organisation, proceed to analyze these documents to find out if any information security aspects are embedded in them.[662] This step will necessitate interviews and discussions with internal auditors, personnel from the human resources department (HR) and people responsible for the drafting of the documents of the organisation.[663] Only after this process has been completed work can start on the development of new policies, standards, procedures and guidelines.

Step 2: Evaluate and develop security policies, standards, procedures and guidelines.[664]

Step 3: Obtain top management support and commitment for the awareness and training program. [665]

One of the biggest and arguably most important challenges is to obtain management support and commitment for the program.[666] Executives must support and be committed to the information security program otherwise it will be abandoned, and widely ignored by all.[667] This step would involve the development and scheduling of a training session targeted at executive-level management. [668] The purpose of this training session is not only to educate executives on the subject-matter of information security, but also to gain their support for it.[669] In order to obtain management's support the internal hierarchy existing within the organisation must first be determined. [670]

---

662 (n 635) 10.
663 ibid.
664 (n 643) 5.
665 (n 495) 318.
666 (n 495) 326.
667 Voss "The ultimate defense of depth: security awareness in your company" (last visited 31 March 2003) http:// www.sans.org/rr/aware/utlimate.php 2.
668 (n 643) 6.
669 ibid.
670 (n 635) 17-18.

When attempting to "sell" information security to management a presentation should be developed that is centered around the following information:

(i) "Nature and size of project;
(ii) Identify business needs it will meet;
(iii) Point out impact of not going forward with project state probable cost;
(iv) Cite estimated losses if not implemented;
(v) Show how you would reach ultimate goal; and
(vi) Allow for questions and answers and be prepared."[671]

The following four factors need to be kept in mind when attempting to gain top management support and commitment for the program:

(i) Communication

Keep in mind that managers are only concerned with costs. Therefor the message to managers must be articulated in business terms that managers understand and are interested in. [672] Top management will only support the program if they are convinced it will succeed.[673]

(ii) Meetings

Certainty must be obtained regarding three issues before walking into a meeting:

(a) Know the business;[674]
(b) Know what management desires;[675] and
(c) Know the technical requirements.[676]

---

671 (n 635) 34.
672 (n 495) 304.
673 (n 635) 30.
674 (n 495) 307.
675 ibid.
676 ibid.

Be able to answer the following questions:

(a) What are management's' concerns? [677]

(b) What are the organisational accomplishments? [678]

(c) How can I improve the long-term strategic plan? [679]

(iii) Education

In stark contrast to the education of employees executives need full disclosure on all potential vulnerabilities that may be exploited and/or threats that may materialise.[680] They must furthermore be educated on the costs associated with information security, as well as the benefits and detriments attached to this discipline.[681]

(iv) Motivation

The following motivational "tools" will impel managers to support the program:

(a) Money. Anything that reflects positively on the bottom line will be supported by management; [682]

(b) FUD (fear, uncertainty and doubt) functions as a major motivational tool. [683] Specifically the fear of damage to the organisation's reputation, in the form of deleterious publicity; [684]

(c) The knowledge on the part of management that they are obliged in terms of a statute, regulation and/or contract to perform a certain act will proof to be a powerful motivational tool for managers;[685]

---

677 ibid.
678 ibid.
679 ibid.
680 (n 3) 152.
681 ibid.
682 (n 495) 311.
683 ibid.
684 (n 495) 313.
685 (n 495) 312.

(d) Sustaining the existing level, and/or increasing the levels of productivity in the organisation;[686] and

(e) Compliance with their duty of due care.[687]

If managers can demonstrate:

(1) security controls and recovery plans have been deployed that are comparable to those found in similar organisations, therefor the organisation has an effective disaster recovery plan in place;[688]

(2) a comparable investment in business continuity and information security have been made, or else[689]

(3) the organisation has documented a good reason for not doing so,[690]

they have fulfilled their obligation of due care.

After initial buy-in from management the second challenge is maintaining management's commitment. [691]

Apart from the commitment and support of senior management, the effectiveness of any information security awareness and training program will furthermore dependent on the long-term appropriation of resources and funding. [692] From preceding chapters it should be clear that most benefits delivered by information security are of an intangible nature, and therefor inherently hard to place a monetary value on.[693] The general formula used to calculate the value of such a benefit would be to deduct the cost of an investment in awareness and training

686 ibid.
687 ibid.
688 (n 495) 313.
689 ibid.
690 (n 495) 314.
691 (n 495) 303.
692 (n 3) 147.
693 (n 3) 148.

from the estimated cost of losses or damages that would have been incurred if the aforementioned investment was not made.[694]

When management makes decisions pertaining to the budget and the allocation of funding, directors and top management will take the following into consideration:

(a) "Number of locations and users in the organisation;
(b) Classifying attendance as mandatory;
(c) Inclusion of third party service providers, consultants, temps;
(d) Cost of conferences, seminars, lectures, magazines;
(e) Security campaign items available for purchase such as cups, id card holders, magnets, hats;"[695] and
(f) Target both existing and new employees and the different levels of the organsation.[696]

Step 4: Determine who the target audience is that will be addressed on the subject-matter.[697] "To be successful, the awareness program should take into account the needs and current level of training and understanding of the employees and management. "[698]

This can be done by:

(i) "Assess the current level of computer usage;
(ii) Determine what the managers and employees want to learn;
(iii) Examine the level of receptiveness to the security program;
(iv) Map out how to gain acceptance; and
(v) Identify possible allies."[699]

---

694 (n 3) 149.
695 (n 3) 147-148.
696 (n 3) 148.
697 (n 643) 9.
698 (n 48) 201.
699 ibid.

When focussing on your target audience apply the **AUDIENCE – principle:**[700]

Analysis:	Who are they, how many will there be?
Understanding:	What is their knowledge of the subject?
Demographics:	What is their age, gender, educational background?
Interest:	Why are they there? Who asked them to be there?
Environment:	Where will I stand? Can they all see and hear me?
Needs:	What are their needs? What are your needs as speaker?
Customise:	What specific needs do you need to address?
Expectations:	What do they expect to learn or hear from you?

Even before the training of employees commences the very first step should be to focus on the selection and appointment of suitable candidates.[701] An investigation should therefor be launched into the background and history of the prospective employee, while simultaneously taking into consideration factors that might influence his/her attitude towards the organisation. [702] Keep in mind that previous employers seldom provide an honest account of how they experienced the candidate.[703]

Only after the organisation has identified and appointed competent and suitable personnel can the issue of training be addressed. When the new employee is employed it is recommended that he or she undergo preliminary training.[704] Furthermore employees who were employed by the organisation before the implementation of the information security awareness and training program must also undergo refresher training.[705]

---

700 Hall "Selling security to management" (last visited 31 March 2003) http://www.sans.org/rr/aware/selling_sec.php 3.
701 (n 4) 123.
702 ibid.
703 ibid.
704 (n 3) 150.
705 ibid.

There are three **major constituencies that influence security effectiveness**,[706] namely end-users, line managers (IT managers) and top management. "The effectiveness of a comprehensive security program is dependant on the degree to which the key enterprise constituencies understand and embrace it."[707]

(i)	**Group:**	**Top management**[708]
Focus of group:		"Expect a sound rational approach to information security. Interested in the overall cost implementation the policies and procedures and how this program stacks up against others in the industry."[709]
Style:		Professional and intellectual, but never threatening. [710]
Schedule:		At least on a quarterly basis. [711]
Best technique:		Cost justification; [712] Industry comparison; [713] Audit report; and [714] Risk analysis [715]
Best approach:		Presentation; [716] One-on-one session; [717]

[706] Tudor is of the opinion that the awareness and training program focuses on five different groups, namely system administrators ("participate in security technical training for the operating system, network, database, or application that he or she manages"); security liaisons; security officers ("need to focus on the information security architecture and its components and how these components are integrated into the security awareness and training program"); department management ("additional responsibility of ensuring all employees within its span of control understand and adhere to security policies and receive security awareness training" also responsible for information classification in their business unit.); and executive management ("must make decisions relating to information security awareness and training and will be responsible for the long-term financial commitment to the program") Tudor (n 3) 146-147; 153.

[707] Meta Group "Do not forget the marketing principles in your security program" (last visited 24 July 2002) http://www.cio.com 4

[708] (n 48) 208.

[709] (n 643) 208.

[710] (n 48) 208.

[711] ibid.

[712] ibid.

[713] ibid.

[714] ibid.

[715] ibid.

[716] ibid.

[717] ibid.

Video;[718] and

Violation reports.[719]

Expected results: Funding and support.[720]

(ii) Group: Line management

Focus of group: "Focused on getting their job done. Will not be interested in anything that will slow them down. To win them over show how controls will improve their job performance."[721]

Style: Informative, collegial and receptive. [722]

Schedule: Monthly, no less.[723]

Best technique: Demonstrate job performance benefits; [724] and

Perform security reviews.[725]

Best approach: Presentation;

Circulate news articles; [726]

Videos;[727] and

Rely on existing; and communication vehicles.[728]

Expected results: Support; [729]

resource help; and

adherence.[730]

(iii) Group: Users/ employees

Focus of group: Will encounter some reluctance.

---

[718] ibid.
[719] ibid.
[720] ibid.
[721] ibid.
[722] ibid.
[723] ibid.
[724] ibid.
[725] ibid.
[726] ibid.
[727] ibid.
[728] ibid.
[729] ibid.
[730] ibid.

> "Identify what is expected of them and how it will assist them in gaining access to information and systems they need to complete their tasks. Point out that by protecting access to information they can have reasonable level of assurance that their information assets will be protected from unauthorised access, modification, disclosure or destruction."[731]

Style:	Can include elements of seriousness and fear, but also fun and concern. [732]
Schedule:	Annual updates[733]
Best technique:	Sign responsibility statements;[734] and Policies and procedure. [735]
Best approach:	Presentation; Newsletters; [736] Video or live presentations; [737] and Policy booklets and posters. [738]
Expected results:	Adherence and support.[739]

As should be evident from the above the training of employees and that of top management differs. When training and educating employees guard against making security breaches and incidents seem inviting and challenging. [740] Furthermore, adopt a need-to-know philosophy, also referred to as the principal of least privilege. [741] Thereby only telling them what they need to know in order to perform their duties effectively and efficiently. [742] Do not educate employees on

731 (n 48) 209.
732 (n 48) 208.
733 ibid.
734 ibid.
735 ibid.
736 ibid.
737 ibid.
738 ibid.
739 ibid.
740 (n 3) 151.
741 (n 516) 6.
742 (n 3) 151.

how to hack or break into systems, because they may view this as an invitation.[743] It is recommended that reference to web sites that supply hacking tools and tips should be omitted. [744] Deter them by explaining the dire consequences that will ensue if they violate any of the security policies or procedures.[745]

To gain a better understanding of what influences each of these constituencies it is recommended that a (SWOT) strength, weaknesses, opportunities and threats analysis is performed:[746]

(i) **Strengths**: In what way do they think well of information security?

(ii) **Weaknesses**: In what way do they think poorly of information security?

(iii) **Opportunities**: What are the best opportunities for information security? and

(iv) **Threats**: What issues could undermine information security?

Step 5: Message creation - obtain certainty regarding the message the organisation wants to convey to their target audience. [747] This step will entail obtaining clarity regarding the objectives of the information security awareness and training program.

The **content** of the awareness and training program will differ depending on the target audience. [748] "Not everyone needs the same degree or type of information security awareness to their jobs." [749] An awareness program that distinguishes between groups of people, and presents only information that is relevant to that

743 ibid.
744 ibid.
745 ibid.
746 (n 707) 4.
747 (n 643) 9.
748 (n 643) 203.
749 ibid.

audience and their job description will have the best results.[750] Consequently segmentation must take place. [751] This would imply segmenting the audience by, for instance:

(i) Level of awareness

Divide employees according to their current level of awareness of the information security objectives. [752]

(ii) Job category

Divide employees according to their job functions or titles:

(a) Senior management;
(b) Middle management;
(c) Line supervisors;
(d) Employees; or
(e) Others.[753]

(iii) Specific job function

Employees may be grouped according to the specific functions they perform or services they deliver:

(a) Service providers;
(b) Information owners; or
(c) Users. [754]

(iv) Information processing knowledge

Determine the level of knowledge that employees on different levels have of computers. [755]

---

750 ibid.
751 ibid.
752 ibid.
753 ibid.
754 ibid.
755 ibid.

(v) Technology, systems, or applications used

Divide the audience based on the technology they use.[756] (eg. MAC users and Intel users).

Course curriculum of the information security awareness and training program will generally addressed the following issues:

(i) Identify and explain the threats facing the organisation; [757]

(ii) Security monitoring program;[758]

(iii) Security policy;[759]

(iv) Information classification and handling;[760]

(v) User ID and password requirements;[761]

(vi) Virus scanning and reporting;[762]

(vii) Shoulder surfing;[763]

(viii) Social engineering;

(ix) System access;[764]

(x) Software license;[765]

(xi) Internet use;[766]

(xii) E-mail use;[767]

(xiii) Physical security of notebooks;[768]

(xiv) Internal network protection;[769]

---

[756] (n 643) 204.
[757] (n 3) 145.
[758] ibid.
[759] ibid.
[760] Kaur "Introducing and education of information security policies to employees in my organisation" (last visited 31 Mach 2003) http://www.sans.org 2.
[761] (n 3) 145.
[762] ibid.
[763] ibid.
[764] (n 760) 2.
[765] ibid.
[766] ibid.
[767] ibid.
[768] ibid.
[769] ibid.

(xv) Release of information to third parties;[770]

(xvi) Use of encryption;[771]

(xvii) Individual responsibilities;[772]

(xviii) Incident reporting;[773]

(xix) Internet access guidelines;[774]

(xx) Information transmission, storage and processing;[775]

(xxi) Information security program;[776]

(xxii) Describe what the organisation is trying to protect and why;[777]

(xxiii) Physical security awareness;[778]

(xxiv) Technical security awareness;[779]

(xxv) Access control;[780]

(xxvi) Business continuity and disaster recovery;[781]

(xxvii) Identify the security team;[782]

(xxviii) Discuss the correct procedure from the moment a security incident has occurred;[783]

(xxix) Password management;[784] and

(xxx) Appropriate use of resources.[785]

Step 6: Evaluate and consider communication tools available to get the security message

---

770 ibid.
771 (n 3) 153.
772 ibid.
773 ibid.
774 ibid.
775 ibid.
776 ibid.
777 (n 667) 4-6.
778 ibid.
779 ibid.
780 ibid.
781 ibid.
782 ibid.
783 ibid.
784 ibid.
785 (n 3) 145-146.

across.[786] Launch an investigation into current training trends. [787] The style and method of training will depend on the nature of the organisation. [788]

Tools that may be used to get the information security message across: [789]

(i) Outside speakers;

(ii) Videos[790] and multimedia presentations;[791]

(iii) Company and departmental newsletters with information such as, who the security team is, what their mission is, references to developments or amendments in security policy and/or programs;[792]

(iv) Contests and drawings;

(v) Create an online information security awareness and training test/quiz;[793]

(vi) Screensavers;

(vii) Information security web site;

(viii) Security brochures and magnets;

(ix) Banner page showing the information security tip of the day;[794]

(x) Posters, cups, calendars, key chains (reminders); [795]

---

786 ibid.

787 (n 48) 201.

788 (n 48) 206.

789 For more ideas on tools to get the information security message across visit http://awarenessmaterials.homestead.com/ . Included in their suggestions are:

(i) First aid kids with the slogan: "It's healthy to protect your patience's information; it's healthy to protect your information."

(ii) Mirror with slogan "Look who is responsible for protecting your information."

(iii) Toothbrush with slogan: "Your password is like this toothbrush; use it regularly, change it often, and do not share it with anyone else.

(iv) "Badge holder retractable with slogan: "Think Security."

(v) Key-shaped magnet with slogan: "You are the key to good security."

(vi) Flashlight with slogan: "Keep the spotlight on information protection."

790 Commonwealth films (www.commonwealthfilms.com) have a variety of information security videos available under the information and computer security section Kaur (n 760) 3.

791 (n 48) 204.

792 (n 48) 205.

793 For more information on how to develop and implement such a test/quiz within your organisation visit http://www.sans.org/rr/aware/quiz.php.

794 (n 495) 320.

795 ibid.

(xi) Distribution of security alerts;

(xii) Intranet;

(xiii) Broadcast voicemail;

(xiv) Computer security day activities;

(xv) Information security handbook;[796]

(xvi) Full-blown PR campaigns[797] Hire a professional PR company to develop and implement the information security program;[798]

(xvii) Corporate magazine;[799] and

(xviii) One of the most effective methods to get the information security message across is to "display readout at entrance to the company restaurant showing the results of the different departments."[800]

Irrespective of which tool is used "the effectiveness of the medium will depend on how well it is created and how succinct the message is."[801]

Step 7: Follow-through with program.[802] An information security awareness programs is often developed and implemented with a certain degree of enthusiasm, unfortunately once the implementation process is complete, the enthusiasm fades away. [803] It must however be realised that information security awareness and training is a continuous process with no end destination in sight. [804] It is therefor essential to develop ways in which to keep the program "alive and growing." In order for the awareness campaign to be successful its message must be communicated repeatedly. [805]

---

796 (n 48) 204.
797 (n 632) 80.
798 ibid.
799 ibid.
800 ibid.
801 (n 48) 205.
802 (n 48) 200.
803 ibid.
804 ibid.
805 (n 495) 320.

Three critical success factors of the program are:

(i) "Tell them what you are going to say;
(ii) say it; and
(iii) remind them of what you have said." [806]

Analogous to other programs operating within the organisation the awareness and training program must be monitored and evaluated[807] on a regular basis.[808] When performing an evaluation of the program consideration must be given to whether or not the original objectives and goals of the security awareness program have been achieved.[809]

By evaluating effectiveness of the awareness and training program the following will be measured:[810]

(i) "The extend that conditions were right for learning and the learner's subjective satisfaction;
(ii) what a given student has learned from a specific course;
(iii) a pattern of student outcomes following a specific course; and
(iv) the value of the class compared to other options in the context of an organisation's overall [information] security training program."[811]

6.3.6.3 Impediments to the program

(i) In most organisations "security is implemented as an afterthought". This results in: (a) employees having to overcome the bad habits they have already learnt, and (b) employees having to be educated

[806] (n 48) 206.
[807] For examples of practical ways in which to evaluate the information security awareness and training program, consult Tipton and Krause (n 495) 322 – 323.
[808] (n 495) 322.
[809] (n 495) 323.
[810] ibid.
[811] ibid.

on how and why information security is of such crucial importance; [812]

(ii) Information security is still viewed as an IT problem. Therefor the need exist to tie information security to every employee's job; [813]

(iii) Awareness and training programs imitate the programs of competitors, or companies in a similar fields. The program must be tailor-made for the organisation it is going to be used in; [814]

(iv) Guard against over educate the audience; [815]

(v) Failure to maintain the program; [816]

(vi) Lack of management support; [817]

(vii) Lack of resources; [818] and

(viii) Most employees still view information security as an inhibitor of performance and productivity. Therefor security and productivity must have equal force within the organisation resulting in a sustainable, workable equilibrium. [819] "Where information security programmes overextend themselves they become burdensome and impede the productivity of the user community." [820]

6.3.6.4 Conclusion

Traditionally information security was viewed by top management as a necessary evil. With the advent of the information age management is beginning to realise that information security is a business enabler, rather than a business inhibitor. [821] It is

---

812 (n 643) 3 - 4.
813 ibid.
814 ibid.
815 ibid.
816 ibid.
817 ibid.
818 (n 495) 322.
819 (n 668) 3.
820 Ludwig "Security awareness: preventing a lack of security consciousness" (last visited 31 March 2003) http://www. sans.org 2.
821 (n 472) 149.

therefor important that any information security program should first review the business objectives of the organisation and ensure that these goals are being met. [822]

> "Meeting the business objectives of the organisation and understanding the customer's needs are what the goal of a security program is all about. An awareness program will reinforce these goals and will make the information security program more acceptable to the employee base." [823]

OUTCOMES DELIVERED BY STEP 6:

An effective information security awareness and training program will:

> "…reduce the risk of loss of corporate information assets by training employees to understand:
>
> (i) the value of information security;
>
> (ii) to recognize their responsibility to protect it ; and
>
> (iii) recognise potential violations and report them." [824]

[822] (n 48) 198.
[823] ibid.
[824] (n 3) 160.

STEP 7: MONITOR AND MAINTAIN

OBJECTIVE OF STEP 7:

This step has as its objective the evaluation, monitoring and maintenance of information security within the organisation on a continuous basis.

Because of the fact that risks and threats change at such an alarming rate it is important to ensure that risks to information security are monitored on a regular basis in order to determine if: (i) the organisation has adequate protection against them, and (ii) if any policies should be amended or controls updated in order to stay effective. [825] Monitoring activities may take an active[826] or passive[827] form, and must form part of the day-to-day operations.[828]

The following **monitoring tools** may be identified:

(i) Internal and external audits;

(ii) Regular investigations;

(iii) Regular reporting and review; and

(iv) Organisational management reviews. [829]

---

825 (n 8) 60.

826 Active activities would encompass the day-to-day monitoring of activities planned and executed by the organisation. Cazemier (n 632) 23.

827 Passive monitoring activities would include, but are not limited to periodical reviews of compliance with best practice. Cazemier (n 632) 23.

828 (n 632) 23.

829 (n 8) 59.

The monitoring step would require that the following activities are performed:[830]

(i) Testing the effectiveness of controls implemented[831]

This exercise will usually be performed by auditors, but the central security group may also perform their own independent tests and compare their results to that of the auditors.[832]

(ii) Monitor compliance with policies, guidelines and standards

Self-assessment tools may successfully be implemented here. [833]

(iii) Build a database of vulnerabilities, threats and risks the organisation have been exposed to in the past

This database will enable the oganisation to first of all calculate the frequency of attacks, violations and damage suffered, and secondly justify future investments in security. [834] To devise a more effective functioning of the database organisations may choose to categorise the threats they have fallen victim to in the past, for instance denial of service, data compromise, unauthorised access, viruses.

Maintenance of information security is increasing in importance due to the ever-changing landscape in which information technology and the business operates.[835]
Problems experienced when performing maintenance include: (i) it is considered to be tedious, inert and unchallenging; and (ii) the maintenance activity can become very

---

830 See Annexure N for an information security governance checklist to ensure that the organisation have sufficiently dealt with all of the aspects this discipline entails.
831 Penetration testing may proof to be helpful when performing this activity. For a detailed discussion on penetration testing refer to phase 3 "vulnerability identification" above.
832 (n 8) 54.
833 (n 8) 55.
834 (n 8) 56.
835 (n 33) 8.

complex requiring the expertise of a specialist.[836] The maintenance function only commences once the design, implementation and monitoring phases are in place.[837]

OUTCOME OF STEP 7:

(i) An effective maintenance and monitoring system that demands from all employees, renewed commitment to information security efforts on a daily basis.

6.3.8 Conclusion

The holistic nature of information security governance is clearly visible when considering the multitude of issues that need to be addressed when wanting to implement information security governance. By following the suggested seven-step plan organisations may rest assured that the most important aspects of information security governance have been considered and are addressed.

It is acknowledge that the initial development, implementation and execution of information security governance are time and resource consuming. Furthermore, it should be kept in mind that maintenance of information security is just as important as developing it in the first place, and might in fact be harder to achieve. It is therefor understandable that some directors might feel that the time, money and effort required for the implementation of this discipline are not justified. However, as will be evident from the discussion in the next chapter, directors that reason like this, are making a deleterious, and potentially very costly mistake.

---

836 (n 12) 36.
837 (n 12) 565.