THE EFFECTIVE IMPLEMENTATION OF INFORMATION SECURITY IN ORGANIZATIONS

Oliver André Hoppe [a] , Johan van Niekerk [b] and Rossouw von Solms [c]
[a] *Port Elizabeth Technikon, South Africa,* oliver@petech.ac.za
[b] *Port Elizabeth Technikon, South Africa,* johanvn@petech.ac.za
[c] *Port Elizabeth Technikon, South Africa, rossouw@petech.ac.za*

Abstract: Due to the overwhelming complexity in establishing and maintaining a secure organizational framework, it is essential that various Information Security Management elements be tightly integrated to form a well planned methodology. However, organizations often do not have the necessary expertise or resources to follow such a detailed methodology. This paper introduces a software tool that can automate the phases comprising the Information Security Management Methodology.

Key words: Information Security Management, Top Management Commitment, Information Security Policies, Risk Management, Security Controls, Information Security Standards, Information Security Toolbox

1. INTRODUCTION

During the last few decades the use of information technology (IT) has become more widespread in all areas of society, and the types of activities that it performs or supports, have become increasingly more important. As a result, information systems are now heavily utilized by all organizations and relied upon to the extent that it would be impossible to manage without them (Hutchinson & Warren, 1999, p. 42).

Loss of confidentiality, integrity, availability, accountability, authenticity and reliability of information and services can have adverse impacts on organizations (GMITS Part 2, 1996, p. 6). Consequently, there is a critical need to protect information and to manage the security of information

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*

technology systems within organizations. This requirement to protect information is particularly important in today's environment because many organizations are internally and externally connected by networks of IT systems (GMITS Part 2, 1996, p. 6). In order to protect the well being of the organization in conducting its business affairs and activities, security must be an integral part of an organization's overall management plan (GMITS Part 1, 1995, p. 2).

As the role of computers and the importance of information have changed, obvious changes have occurred in the risks posed to computers and information (Forcht, 1994, p. 373). A new view of organizational security must be taken, in which protecting information is a *proactive, planned and designed* action rather than a reaction to technology changes in the organization. As a result, it is essential that organizations follow a structured methodology when implementing and maintaining an Information Security Management System.

2. INFORMATION SECURITY MANAGEMENT

To manage, that means to introduce and maintain, a secure IT environment calls for a comprehensive IT security programme (Von Solms, 1998, p. 221). A systematic approach is required for the identification of requirements for, the implementation of, and administration of IT security within an organization. This process is termed the management of IT security (GMITS Part 1, 1995, p. 7). IT security planning and management is the overall process of establishing and maintaining an IT security programme within the organization. It encompasses people, processes and IT systems. Because management styles and organizational sizes and structures differ, this process should be tailored to the environment in which it is used. (GMITS Part 2, 1997, p. 2). As a result, it is essential that organizations follow a structured methodology that is based upon sound principles and management procedures, when implementing and maintaining an Information Security Management System (ISMS).

3. ELEMENTS OF INFORMATION SECURITY MANAGEMENT

One of the key elements of the philosophy of an Information Security Management System is that it is based on a principle of integration. The development of an integrated methodology can best be achieved by studying the elements that are necessary for the introduction of an *integrated* security management methodology. These elements will be discussed in the subsections to follow.

3.1 Top Management Commitment

Top management is the legal owner of all information in the organization and is ultimately responsible for the protection of this information (Forcht, 1994, p. 379). This indicates that one of the fundamental steps towards achieving the successful implementation and maintenance of an Information Security Management System is that of gaining top management commitment. There are several reasons for this.

Firstly, top management support is required for financial backing of such a project. The reality is that the development and implementation of this project will require funding and that top management will have to be the source of this funding.

Also, commitment from top management will result in greater support being gained from the entire organization. This is important, as in many organizations the general employees traditionally have felt a certain level of opposition towards the IT department. If they feel that this is an organizational project, rather than an IT department project, they are more likely to support it, and will, thus, also show a greater respect for the security initiatives devised.

Clearly, without the benefits provided by gaining top management support, the introduction of an effective Information Security Management System will be nearly impossible. For this reason, gaining top management support is one of the critical factors in the preparation for the introduction of information security management. The commitment of top management to IT security is critical and should take the form of a formally agreed upon and documented corporate information security policy (GMITS part 2, 1996, p. 10).

3.2 Information Security Policy

The information security policy is a document with the purpose of providing management support and direction for information security (BSI, 1995, p. 3). Policies describe management requirements at a high level, stating "what is required" and not "how to do it" (Moule and Giavara, 1995,

p. 13). The IT security policy describes the approach to dealing with the security problems faced by the organization. It should be based on the IT security objectives and strategies (GMITS Part 3, 1997, p. 9).

As mentioned, top management communicates through policies and procedures. It is therefore imperative that the information security policy provides guidance concerning both the implementation of information security as well as follow-up activities. In addition, by having the different areas of the organizations comply with a single information security policy, the groundwork is put in place for an integrated implementation of information security management (Vermuluen, 2001, p. 97).

The policies must be implemented by a application of appropriate safeguards to the systems and services to ensure that an adequate level of protection is achieved. (GMITS Part 2, 1996, p. 18).

3.3 Information Security Controls and Procedures

The previous section highlighted the fact that the information security policy is a document containing high level statements that describe the organization's security requirements. These high level statements or policy statements refer to the appropriate security countermeasures that actually implement information security. These security controls are carried out by following a series of operational steps called procedures (Wood, 1994, p. 12).

It is apparent that a hierarchical relationship exists between security policy statements, security controls, and security procedures. At the top of the hierarchy are the security policy statements, which are implemented by a set of security controls. The objectives of these controls are achieved by following a series of security procedures. However, before a security policy can be drawn up it is necessary to identify the security controls that are best suited towards addressing the information security needs of the organization. The objective of information security is, therefore, to manage security risks through the identification and implementation of selected security countermeasures.

3.4 Risk Management

The purpose of risk management is to identify the security countermeasures to a level justified by the analysed measures of risk; in order to reduce to an acceptable level the chances of the type of the event recounted occurring (Halliday, 1995, p. 70).

Risk management embodies a number of different risk management approaches that can assist in identifying and implementing security controls for the organization. In the past, there were two approaches that were often used by organizations to identify the security controls that were to be installed (GMITS Part 3, 1997, p. 11).

Traditionally, organizations have used risk analysis to accomplish this task. With risk analysis, assets, threats and risks are given weighted values, which are used to determine which controls are necessary for their protection. This process is both time consuming and expensive.

An alternative to traditional risk analysis is the baseline approach. This is an approach where documentation is consulted which contains a comprehensive set of the minimum security requirements which should be present in an organization. The most prominent current example of this approach is the Code of Practice for Information Security Management (BS 7799) (Guide to the CoP, 1995, p. 5).

When undertaking one of the aforementioned risk management strategies, it is essential that organizations consult leading international information security standards. This will assist in providing guidance and insight into the steps required to perform such a multifaceted procedure.

3.5 Information Security Standards

As has been stated previously, the introduction of information security management is a complex process that must be based upon business needs and an integrated process. To gain a better understanding of this process, it may be useful to consult prominent information security standards. Such standards can help organizations by providing them with greater insight into what it is that comprises information security management and what steps are essential to its introduction. Two examples of such comprehensive IT security standards are the Guidelines for the Management of IT Systems (GMITS) and BS 7799.

GMITS is not intended as a solution to the IT security problems of an organization, but rather as a guideline for the implementation of an IT security plan. It is expected that the parties responsible for IT security within an organization should be able to adapt the specifications presented in GMITS to meet their specific needs. (GMITS Part 1, 1996, p. iv).

BS 7799 contains a comprehensive set of controls, which are divided into ten logical groups. These are considered to be a collection of the best information security practices being implemented in leading international companies. As well as detailing essential basic countermeasures, BS 7799 also provides guidance on security policies, staff security awareness, business continuity planning, and legal requirements (Hutchinson & Warren, 1999, p. 43).

Based on the above-mentioned factors, the implementation and management of information security elements requires a disciplined and integrated process. To accomplish this, it is necessary that a well defined approach to employ and maintain information security be adopted by organizations. This paper will not propose a method for achieving this as such a model has already been achieved with the Vermeulen (Vermuluen, 2001) Information Security Management Methodology (ISMM).

4. INFORMATION SECURITY MANAGEMENT METHODOLOGY

In section three, the components that constitute information security were discussed. The concept of an Information Security Management System was introduced. It was determined that an Information Security Management System is required for the effective implementation and maintenance of information security within an organization. The section concluded by necessitating the need for the integration of the various information security components. It was suggested that a methodology be developed which would assist in meeting the complex needs of establishing and maintaining an integrated Information Security Management System.

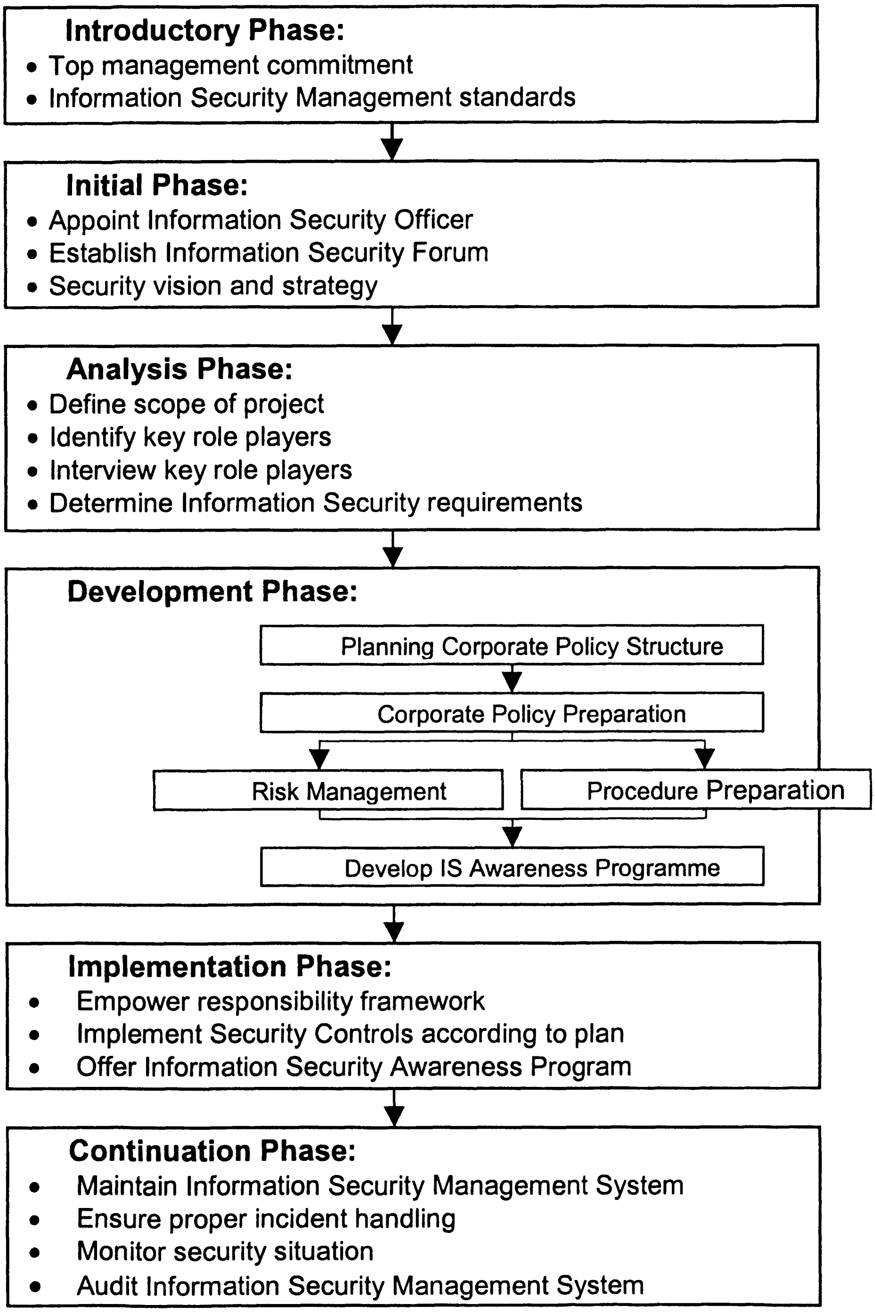
Introductory Phase:
• Top management commitment
• Information Security Management standards
Initial Phase:
• Appoint Information Security Officer
• Establish Information Security Forum
• Security vision and strategy
Analysis Phase:
• Define scope of project
• Identify key role players
• Interview key role players
• Determine Information Security requirements
Development Phase:
Planning Corporate Policy Structure
Corporate Policy Preparation
Risk Management
Procedure Preparation
Develop IS Awareness Programme
Implementation Phase:
• Empower responsibility framework
• Implement Security Controls according to plan
• Offer Information Security Awareness Program
Continuation Phase:
• Maintain Information Security Management System
• Ensure proper incident handling
• Monitor security situation
• Audit Information Security Management System

Figure1. Information Security Awareness Model

The studied methodology, shown in Figure 1 (Vermuleun, 2001, p. 6), is comprised of six phases for the implementation and management of information security, they are:

1) Introductory Phase
2) Initial Phase
3) Analysis Phase
4) Development Phase
5) Implementation Phase
6) Continuation Phase

These phases form an outline for the implementation of information security management. It is, however, necessary to determine the steps required for the completion of each of the phases.

4.1 Introductory Phase

The objective of the Introductory Phase is to put the core elements of information security management into place. These elements comprise the steps that will be necessary to support the entire information security management process, during its implementation and on an ongoing basis. The Introductory Phase is comprised of two steps, they are:

- Gain Top Management Commitment
- Consult Information Security Standards

4.2 Initial Phase

The Introductory Phase was responsible for establishing steps that would contribute towards the introduction of information security. The objective of the Initial Phase is to complete the preparation stage of information security management and allow for its subsequent implementation in the organization.

In the Introductory Phase the responsibility of introducing security has moved to top management of the organization. In the Initial Phase, the implementation of information security has been delegated to lower management (Vermuluen, 2001, p. 115). This can be attributed to the establishment and empowerment of a responsibility framework. Taking this into account, the steps comprising the Initial Phase are:

- Appoint an Information Security Officer
- Establish a Information Security forum
- Define Security Vision and Strategy

Once top management commitment has been obtained, and the appropriate managerial framework has been put into place, the organization has laid the foundation for addressing the information security management needs of the organization.

4.3 Analysis Phase

The Introductory Phase and the Initial Phase have prepared the organization for the implementation of information security management. Having created the foundation for the implementation of information security management, the Analysis Phase begins the process leading up to implementation (Vermuluen, 2001, p. 119). The objective of the Analysis Phase is to determine the security requirements of the organization.

The following steps are proposed as necessary for the accomplishment of the goals of the Analysis Phase:

- Determine Scope of the ISMS
- Determine Key Role Players
- Interview Key Role Players
- Determine Security Requirements

A number of steps are required to determine the security requirements for the organization. Firstly, it is suggested that the areas of the organization that information security management will be applied to, be determined. Having determined this, it is proposed that a high level business analysis be performed by means of interviewing a selection of organization members who act as information owners and custodians (Parker, 1998, p. 298). Once the business analysis has been completed, it is necessary to translate the identified business needs into security requirements.

Once all the above mentioned steps have been successfully completed, the objective of the Analysis Phase has been accomplished, namely to determine the security requirements of the organization. It is now necessary to use the security requirements to plan the effective implementation of information security management. This will form the Development Phase and will be discussed in the following sub-section.

4.4 Development Phase

The Analysis Phase identified the security requirements that define the information security needs of the organization. Before this information can be used to successfully implement security within the organization, proper planning is required to ensure that a well structured process is followed. For this reason the Development Phase of the proposed methodology is required. The objective of the Development Phase is to evaluate the security requirements and use this information to determine in what way information security management will be implemented in the organization.

The following steps are proposed to allow for the accomplishment of the above mentioned objective:

- Planning the information security policy structure
- Information security policy preparation
- Risk management
- Procedure preparation
- Develop an information security awareness programme

Although the ISMM provides a comprehensive and formalised approach towards analysing the security needs of the organization, the methodology lacks detail with regard to the selection of security safeguards. It is therefore recommended that two more selection approaches be incorporated into the Development Phase. The proposed safeguard selection procedures are:

4.4.1 Predefined Security Profiles

This approach provides organizations with a set of predefined security profiles that are based on best information security practices. This allows an organization to select a profile that best accommodates the organizations operational environment. As an example, an academic institution would select an academic security profile, thereby being provided with a set of modifiable security safeguards that are most likely to effectively address the security needs of the institution in question.

4.4.2 Phased Security Levels

Phased security levels allow organizations to implement the proposed set of BS 7799 security safeguards using an incremental approach. Although BS 7799 proposes a minimal set of safeguards, most organizations do not have the necessary resources to implement the full set of safeguards. Security safeguards are therefore distributed across five security levels, with level one providing minimal security and level five providing maximum security by implementing all BS 7799 security safeguards.

By incorporating the proposed approaches into the Development Phase, organizations are provided with three options when selecting security safeguards, namely, selecting security countermeasures based upon *Security Requirements Analysis, Predefined Security Profiles or Phased Security Levels.*

4.5 Implementation Phase

Upon successful completion of the Development Phase, the organization is ready for the implementation of an Information Security Management System. The goal of the Implementation Phase is to implement information security according to the guidelines provided by the documents compiled in the previous phase.

Based upon these activities, the following steps are proposed for the realisation of the Implementation Phase:

- Empower Responsibility Framework
- Implement Safeguards according to plan

Offer Security Awareness programme

4.6 Continuation Phase

The previous five phases have lead up to the implementation of an Information Security Management System within an organization. However, as previously mentioned, it is vital that support be provided throughout the implementation of information security. For this reason, the Continuation Phase is necessary.

The following steps are proposed to fulfil the Continuation Phase:

- Maintain Information Security Management System

- Monitor security situation
- Audit Information Security Management System compliance
- Ensure proper incident handling

The six phases that where described in this section illustrate how an Information Security Management System can be successfully implemented using the proposed ISMM. This is achieved by providing implementation guidance through a structured and phased approach.

However, organizations often do not have the expertise or resources to follow such a detailed methodology. As a result, it can be considered essential to provide a software tool that can automate the phases comprising the ISMM. Such a software tool will be examined and expanded on in the following section.

5. INFORMATION SECURITY MANAGEMENT TOOLBOX

Section four described the process leading to the development of a methodology for the establishment of an Information Security Management System. This methodology proposed an implementation model that was used as the basis for the development of an automated software tool to guide the establishment and preservation of information security management in an organization.

This software package carries the working title of the Information Security Management Toolbox (ISMTB). This package will provide services in assisting information security management.

Various aspects concerning such an automated tool will be examined. Further insight will be provided on how the proposed methodology can be implemented in the form of a software package.

5.1 Technical Design Architecture

The proposed methodology outputs large volumes of sensitive information, as well as automates several activities. It is therefore essential to consider an environment that can accommodate the necessary requirements. Such an environment is the stand-alone desktop environment.

The ISMTB was implemented as a stand-alone desktop application using a three-tier software architecture within a file sharing environment. The primary reason for distributing the application's functionality across multiple tiers was to obtain the benefits of a client/server implementation while executing the ISMTB within a local desktop environment. Having discussed the architectural design considerations, it becomes necessary to examine the internal workings of the ISMTB..

5.2 Mechanics of the Information Security Management Toolbox

The focus of this sub-section is not to provide an overview of all the implemented application functionality, but rather to concentrate on the complex mechanics that were designed to automate the various phases of the proposed ISMM.

Firstly, The Introduction module is responsible for introducing the application users to the concept of information security as well as emphasizing the importance of adhering to a structured and disciplined process when implementing an Information Security Management System. The module was implemented using a hypertext approach, thereby presenting the information as a series of hyperlinked web pages that are installed, with the ISMTB, on the client's local desktop environment.

Although the Introduction module introduces the application users to the concept of information security, it does not provide a means for identifying and proposing a set of security controls to effectively address the security needs of the organization.

This aspect is implemented in terms of an interactive wizard that serves to automate the steps of the Analysis and Development Phases of the ISMM. The primary objective of the wizard is to propose a set of modifiable security safeguards that will aid in addressing the information security needs of the organization. The sub-sections to follow will examine the implementation of the proposed safeguard selection procedures.

5.2.1 Security Requirements Analysis

As mentioned before, it was determined that business requirements may be gained by interviewing a selection of key role players within the organization. These interviews should be performed using a high level business analysis questionnaire. Based upon the outcome of the questionnaire, the security requirements will be determined.

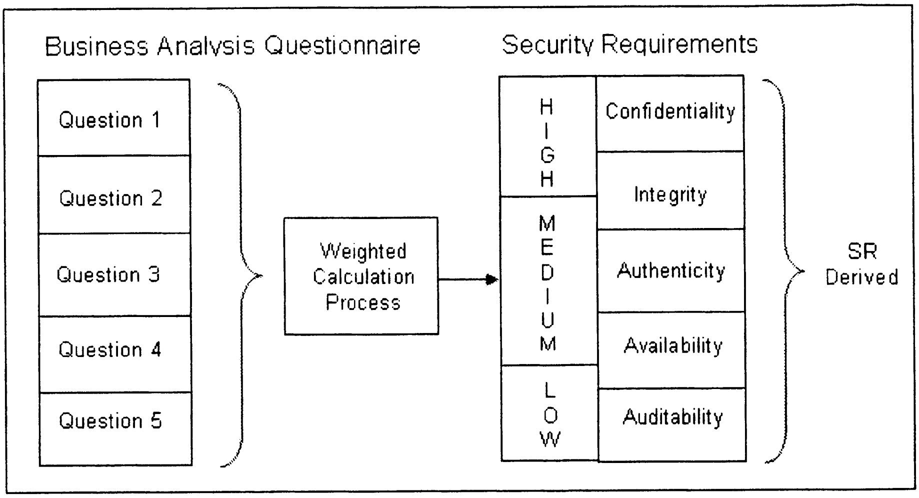

Figure2. Determining Security Requirements from Questions

The business questionnaire is implemented in terms of an automated guide. Each of the questions making up the business analysis questionnaire refers to a specific security requirement. However, to properly assess the importance of security requirements, each security requirement should be referred to by a number of questions in the questionnaire. For this reason, there will be a dependent relationship between security requirements and business analysis questions.

The answers selected for each of these questions will determine what rating (i.e. low, medium or high) each associated security requirement will have. As there is not a direct relationship between the ratings of security requirements and the answers related to each question, a weight value will be attached to each answer of a question, thereby using a calculated process to determine the security requirements for the organization.

Based upon the identified security requirements, a series of modifiable security controls are presented to the organization. These security controls are formulated by means of a lookup matrix which maintains a mapping between the various security requirements and their associated security controls. These safeguards should provide baseline protection such as those proposed in BS 7799 (BS 7799-1, 1999). Each security control contains a set of associated security procedures which serve as a guideline for achieving the objectives of each security control. However, the presented security safeguards merely serve as a lead for implementing information security in accordance to the organizations operational environment. The user is presented with the option of selecting or de-selecting other security controls, provided that a legitimate reason is provided in accordance to the statement of applicability proposed by BS 7799. The elements and relationships representing this process are shown in Figure 2.

5.2.2 Phased Security Levels

The user is prompted to select a security level that best accommodates the security requirements of the organization. Once the appropriate security level has been chosen, a set of predefined modifiable security controls is presented to the organization. As in the Security Requirements Analysis, each security control has several associated security procedures which could be used as a guide when implementing the selected security safeguards. Again, users are presented with the flexibility of adding or removing security controls from other security levels. The mapping between security levels and the associated security controls is depicted in Figure 3.

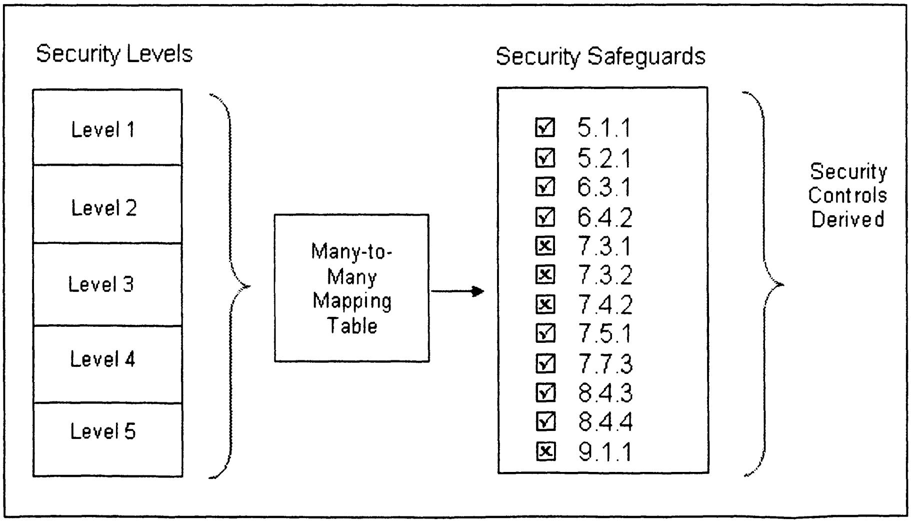

Figure3. Phased Security Level Mapping

5.2.3 Predefined Security Profiles

In essence, this approach operates in the same manner as that of the Phased Security Levels approach. The user is presented with various predefined security profiles and is prompted to select the security profile that best accommodates the security needs of the organization. Once the security profile has been selected, the ISMTB provides a set of modifiable security safeguards that can be adjusted according to the organizations own discretion. Once again, for each modification made to the proposed set of security safeguards, the organization is forced to provide a detailed motivation for deviating from the proposed 'security guidelines'.

All three approaches lead to the proposal of a set of adaptable security safeguards that are intended to serve as a guideline for addressing the information security needs of the organization. Flexibility is provided with regard to the modification of the identified security controls; thereby allowing further customisation based on the organizations unique security requirements. During the process of identifying and selecting security safeguards, the ISMTB dynamically generates the appropriate security documents required to enforce information security.

6. CONCLUSION

Information security is becoming increasingly important as information and the information technology (IT) systems, on which the information is processed, become important business assets. IT systems have become the backbone of most organizations. At the same time computer systems have become open and accessible to others. As a result, it is essential that organizations follow a structured methodology when implementing and maintaining information security.

Information security may, however, be implemented and maintained more effectively in an organization if it is introduced in the form of a complete Information Security Management System. This suggests the need for a structured methodology to provide guidelines for the establishment of information security. Such a methodology, namely the Information Security Management Methodology (ISMM), has been studied.

The nature of the ISMM allows it to be implemented in the form of an automated software package. This package, the Information Security Management Toolbox, includes content provided by several other research projects. The ISMTB serves as an electronic aid providing both interactive elements and textual guidance. This will assist in ensuring the realisation of the proposed ISMM, thereby effectively addressing the identified security requirements of the organization in a structured and integrated manner. .

7. REFERENCES

BS 7799-1. (1999). Information security management - Part 1: Code of practice for information security management. London: British Standards Institution.

British Standards Institute (1995). Guide to the British Standard Code of Practice for Information Security Management. PD 0007, United Kingdom.

Forcht, K.A. (1994). Computer Security Management. Massachusetts: Boyd & Fraser.

Guidelines to the Management of Information Technology Security (GMITS). (1995). Part 1, ISO/IEC, JTC 1, SC27, WG 1.

Guidelines to the Management of Information Technology Security (GMITS). (1996). Part 1, ISO/IEC, JTC 1, SC27, WG 1.

Guidelines to the Management of Information Technology Security (GMITS). (1996). Part 2, ISO/IEC, JTC 1, SC27, WG 1.

Guidelines to the Management of Information Technology Security (GMITS). (1996). Part 3, ISO/IEC, JTC 1, SC27, WG 1.

Guidelines to the Management of Information Technology Security (GMITS). (1997). Part 2, ISO/IEC, JTC 1, SC27, WG 1.

Guidelines to the Management of Information Technology Security (GMITS). (1997). Part 3, ISO/IEC, JTC 1, SC27, WG 1.

Halliday, S. & Von Solms, R (1995). An Alternative Approach to IT Risk Analysis and Management. MTech thesis. Port Elizabeth : Port Elizabeth Technikon.

Hutchinson, B. & Warren, M. (1999). The Future of Australian & New Zealand Security Standard AS/NZA 4444? In J.H.P. Eloff & L. Labuschagne & R. von Solms & J. Verschuren

(Eds.). Information Security Management & Small Systems Security (pp. 41 - 49). United States of America : Kluwer Academic Publishers.

Moule, B. & Giavara, L. (1995). Policies, procedures and standards: an approach for implementation. Information Management & Computer Security, 3, (3). pp. 12-16.

Parker, D.B. (1998). Fighting computer crime: a new framework for protecting information. New York: John Wiley & Sons, Inc.

Von Solms, R. (1998). Information Security Management (3): the Code of Practice for Information Security Management (BS 7799), Information Management & Computer Security, 6 (5), pp. 224-225.

Vermeulen, C. & Von Solms, R (2001). The Development and Implementation of a Methodology for an Integrated Information Security Management System in an Organization. Unpublished MTech thesis. Port Elizabeth : Port Elizabeth Technikon.

Vermeulen, C. & Von Solms, R (2001). Information Security Management Toolbox – Taking the pain out of Security Management.

Wood, C. Charles. (1994). Information security policies made easy: A comprehensive set of information security policies.