

**AN INFORMATION SECURITY RETRIEVAL AND  
AWARENESS MODEL FOR INDUSTRY**

**ELMARIE KRITZINGER**

**AN INFORMATION SECURITY RETRIEVAL AND  
AWARENESS MODEL FOR INDUSTRY**

**by**

**ELMARIE KRITZINGER**

**submitted in accordance with the requirements**

**for the degree of**

**DOCTOR OF PHILOSOPHY**

**in the subject**

**INFORMATION SYSTEMS**

**at the**

**UNIVERSITY OF SOUTH AFRICA**

**PROMOTER: PROF. E. SMITH**

**JUNE 2006**

## **ACKNOWLEDGEMENTS**

My heartfelt thanks to my promoter, Professor Elmé Smith, for her creative input and guidance throughout my research project.

I also wish to thank the following people:

- Werner, my loving husband, for his unwavering support and endless patience.
- My father, for this invaluable time and advice.
- My mother, for her constant love.
- Ilse, Jaco, Johan and René for their moral support.

## ABSTRACT

The present study originated from a realisation that employees in an organisation should be aware of their role and responsibility towards securing the information they work with. Only if employees are aware of their role and responsibilities towards Information Security, could they be held accountable if the information they work with is compromised in any way.

Further motivation for the study was the realisation that information is the lifeline of many organisations and should therefore be properly secured and managed to ensure that it is not compromised in any way. If organisations fail to do so, they could be faced with serious consequences such as prosecution under a number of legal frameworks, or a loss of money, time and business opportunities. The ultimate responsibility for the management of Information Security lies with top management. Top management should enforce Information Security and create an Information Security culture within the organisation. To ensure that employees adhere to the Information Security rules and regulations, top management should measure and monitor the status of Information Security awareness among employees on a continuous basis. A further incentive for this study was the realisation that many Information Security breaches occur due to human action (deliberate as well as accidental). Information Security should therefore also address the non-technical, human-related Information Security issues and not focus on the technical issues only.

Bearing these realisations in mind, this study is principally aimed at making a contribution towards enhancing Information Security awareness in industry, and for this reason, culminates in an Information Security Retrieval and Awareness model specifically developed for the industry sector. While developing this model, special care was taken to address the limitations of current models in the said domain.

An investigation into the current status of Information Security awareness in each of the sectors of the Information Security community (i.e. government, industry and academia) indicated that there is an urgent need for enhancing Information Security awareness in each of these sectors. Although many governments around the globe

have initiated projects to address Information Security, they should continue to launch new initiatives to keep up with the constant changes in Information Technology. These changes continuously trigger new risks that could lead to Information Security breaches. In the Industry sector, technical Information Security issues receive most of the attention when Information Security is addressed, and the non-technical, human-related Information Security issues are often ignored or neglected. The pressing need for an Information Security awareness model for industry that incorporates the non-technical, human-related Information Security issues is therefore self-evident. The academic sector has incorporated Information Security into its curricula, but these efforts are still not enough. Information Security should be incorporated at all levels – undergraduate as well as postgraduate – and should be included in Computer Science and Information Systems, as well as other related disciplines such as Law. After having investigated the current status of Information Security awareness in the Information Security community, the researcher proceeded to explore the ongoing development of Information Security over the past few years. These developments created paradigm shifts ranging from a purely technical approach towards Information Security, towards a more managerial way of protecting information, and currently focusing on creating an Information Security culture within organisations.

With the development of Information Security came Information Security documents that address the management and implementation of Information Security. An investigation into these documents has led to the identification of ten Information Security documents that are accepted as leading documents in the Information Security community. These documents were identified as the basis for a Common Body of Knowledge for Information Security suited to industry. After having explored the limitations of current efforts to create such a Common Body of Knowledge, a Common Body of Knowledge for Information Security suited to industry that addresses these limitations was proposed.

The proposed Common Body of Knowledge addresses the Information Security responsibility of both users with little or no formal background on Information Security, and of specialists in the field. This is achieved by grouping stakeholders according to their job category into IT authority levels. The people on each IT authority level have different responsibilities towards securing the information they

work with. In addition, the proposed Common Body of Knowledge explicitly distinguishes between the technical and the non-technical, human-related Information Security issues. Such a Common Body of Knowledge can be used as a guideline during the management and implementation of Information Security in industry.

Having explored the IT authority levels of a typical organisation and after investigating the non-technical, human-related Information Security issues, an Information Security Retrieval and Awareness model (ISRA) was developed specifically for the industry. The proposed model enhances Information Security awareness in the said domain in the sense that it is based on a Common Body of Knowledge for Information Security suited to industry. In addition, the ISRA model ensures that stakeholders are made aware of the Information Security issues relevant to their specific job category only, to prevent them from being burdened with irrelevant information. Finally, the ISRA model allows stakeholders to retrieve specific information related to Information Security at any time.

The ISRA model focuses specifically on the industry sector and consists of three parts: the ISRA Dimensions; Information Security Retrieval and Awareness; and Measuring and Monitoring. The ISRA dimensions form the building blocks of the model and integrate the non-technical, human-related Information Security issues, the IT authority levels and the 10 state-of-the-art Information Security document dimensions. The purpose of the Retrieval and Awareness part of the ISRA model is to enable each stakeholder to retrieve information from the ISRA dimensions at any time. In this way Information Security awareness among all stakeholders can be enhanced. IT authority levels could also request specific information to assist them in their decision-making processes. The last part of the ISRA model, Measuring and Monitoring, provides top management with a tool to determine the status of Information Security awareness within the organisation and enables them to identify vulnerable areas with regard to Information Security awareness.

The current research culminates in the development and implementation of a prototype to confirm that the ISRA model is not merely a theoretical concept, but that it also constitutes a practicable Information Security Retrieval and Awareness model.

# TABLE OF CONTENTS

## Chapter 1: Introduction

1.1	Introduction.....	2
1.2	Motivation for this study.....	3
1.2.1	Information is the lifeline of many organisations and must be protected.....	3
1.2.2	Information Security is a human-related issue.....	4
1.2.3	Lack of Information Security awareness .....	5
1.2.4	Lack of Information Security governance .....	5
1.2.5	Monitoring the enforcement of Information Security.....	6
1.3	Problem statement.....	6
1.3.1	What is the current status of Information Security awareness?.....	8
1.3.2	What is meant by non-technical, human-related Information Security issues? .....	8
1.3.3	What Information Security issues should employees be aware of to enhance Information Security awareness?.....	8
1.3.4	How can one prevent employees from being burdened with unnecessary information?.....	9
1.4	Terminology used in this thesis .....	9
1.4.1	Information Security .....	9
1.4.1.1	Identification and authentication.....	10
1.4.1.2	Authorisation.....	10
1.4.1.3	Confidentiality .....	10
1.4.1.4	Integrity.....	10
1.4.1.5	Non-repudiation .....	11
1.4.2	Availability of information .....	11
1.4.3	Information Security awareness.....	11
1.4.4	Information Security controls .....	11
1.4.5	Information Security governance.....	11
1.4.6	Information Security management.....	12
1.4.7	Information Security plan .....	12
1.4.8	Information Security policies.....	12

1.4.9	Threats.....	12
1.4.10	Vulnerability .....	12
1.5	Thesis layout .....	13

**Chapter 2: Status of Information Security awareness**

2.1	Introduction.....	18
2.2	The state of Information Security awareness in the government sector .....	19
2.2.1	Current Information Security awareness initiatives within the government sector.....	20
2.3	The state of Information Security awareness within the industry sector .....	22
2.3.1	Issues to be addressed when aiming to enhance Information Security awareness in industry .....	23
2.3.1.1	Information Security is a human issue.....	23
2.3.1.2	Employees should not be burdened with unnecessary information.....	24
2.3.1.3	The Board of Directors and Executive Management are ultimately responsible for Information Security awareness.....	24
2.3.1.4	Goal and content of an Information Security awareness programme.....	25
2.3.1.5	Appropriate Information Security awareness programme .....	25
2.3.1.6	Information Security awareness programmes should be measured and monitored .....	26
2.3.1.7	Information Security awareness programmes should be presented regularly .....	27
2.4	The state of Information Security awareness in the academic sector .....	27
2.4.1.1	Prominent research outcomes regarding Information Security awareness in the academic sector .....	28
2.4.1.2	Information Security should form part of undergraduate as well as postgraduate curricula.....	28
2.4.1.3	Information Security is multidisciplinary .....	29
2.4.1.4	Non-technical Information Security issues should also be addressed ....	29
2.4.1.5	Shortage of Information Security educators and professionals .....	30
2.4.1.6	Information Security curricula should adhere to the requirements of government and industry.....	30
2.4.1.7	Information Security curricula should keep up with new developments	31



2.5	Conclusion .....	31
-----	------------------	----

**Chapter 3: Towards a Common Body of Knowledge for Information Security suited to industry**

3.1	Introduction.....	35
3.2	The on-going development of Information Security .....	35
3.2.1	The technical wave .....	36
3.2.2	The management wave .....	37
3.2.3	The institutional wave.....	38
3.3	Information Security documentation .....	39
3.3.1	The Board Briefing Document on IT Governance .....	40
3.3.2	The Commonwealth Protective Security Manual .....	41
3.3.3	The Financial Aspects of Corporate Governance Report (Cadbury Report) .....	42
3.3.4	The Governance, Control and Audit for Information and Related Technology (COBIT) document .....	43
3.3.5	The Information Security Governance: Guidance for Boards of Directors and Executive Management document.....	44
3.3.6	The Information Technology - Guidelines for Management of IT Security (GMITS) document.....	45
3.3.7	The International Organization for Standardization: ISO 17799 and ISO 17799:2005 .....	46
3.3.8	The IT Infrastructure Library (ITIL) on Security Management document... ..	47
3.3.9	The King Report .....	48
3.3.10	The National Institute of Standards and Technology (NIST) Handbook .....	49
3.4	Common Body of Knowledge for Information Security .....	50
3.4.1	A Common Body of Knowledge for Information Security suited to industry .....	50
3.5	Conclusion .....	54

**Chapter 4: IT authority levels**

4.1	Introduction.....	58
4.2	Grouping of stakeholders.....	58

4.3	Information Security responsibilities of IT authority levels .....	62
4.3.1	Board level .....	62
4.3.2	Executive (senior) Management level .....	63
4.3.3	Middle Management level .....	63
4.3.4	Technical Management level .....	64
4.3.5	Information Security Management level .....	65
4.3.6	User level .....	65
4.4	Summary of Information Security responsibilities .....	66
4.5	Conclusion .....	68

**Chapter 5: Non-technical Information Security issues**

5.1	Introduction.....	72
5.2	The non-technical Information Security issues.....	72
5.2.1	Risk management.....	73
5.2.2	Information Security management.....	73
5.2.3	Corporate governance (including Information Security governance) .....	74
5.2.4	Legal issues.....	75
5.2.5	Computer ethics .....	76
5.2.6	Professionalism .....	77
5.2.7	Information Security culture .....	78
5.2.8	Information Security policy .....	79
5.2.9	Physical security .....	80
5.3	Conclusion .....	80

**Chapter 6: Information Security Retrieval and Awareness (ISRA) model – The concept**

6.1	Introduction.....	83
6.2	Scope of the ISRA model .....	84
6.3	Conceptual view of the ISRA model .....	85
6.3.1	Three-dimensional approach.....	85
6.3.2	The ISRA model .....	87
6.4	Conclusion .....	88

**Chapter 7: Information Security Retrieval and Awareness (ISRA) model – The model**

7.1 Introduction..... 91  
7.2 Part 1: ISRA Dimensions..... 91  
7.3 Part 2: Information Security Retrieval and Awareness..... 93  
    7.3.1 y-Slicing..... 93  
    7.3.2 z-Slicing..... 106  
    7.3.3 Combination Slicing ..... 115  
7.4 Part 3: Measuring and Monitoring..... 118  
7.5 Conclusion ..... 119

**Chapter 8: Information Security Retrieval and Awareness (ISRA) model – Implementation**

8.1 Introduction..... 123  
8.2 Scope of the prototype ..... 123  
8.3 Real-life industry-based organisation ..... 125  
8.4 The prototype ..... 126  
    8.4.1 Information Security Awareness Program..... 127  
        8.4.1.1 Board level..... 127  
        8.4.1.2 Executive Management level..... 142  
        8.4.1.3 User level ..... 156  
    8.4.2 Reports ..... 173  
    8.4.3 Information Security Retrieval ..... 177  
8.5 Strengths and limitations of the prototype..... 181  
8.6 Conclusion ..... 182

**Chapter 9: Conclusion**

9.1 Introduction..... 186  
9.2 Research overview ..... 186  
    9.2.1 What is the current status of Information Security awareness?..... 186

9.2.2	What is meant by non-technical, human-related Information Security issues?	187
9.2.3	What Information Security issues should employees be aware of to enhance Information Security awareness?	188
9.2.4	How can one prevent employees from being burdened with unnecessary information?	189
9.3	Pros and cons of the ISRA model	189
9.4	Future research	191
	References	192
	<b>Appendix A: Specifications for a prototype for the Information Security Retrieval and Awareness (ISRA) model</b>	<b>A-1</b>
	<b>Appendix B: Prototype user's guide</b>	<b>B-1</b>
	<b>Appendix C: Paper presented at the Learning Conference, London UK, June 2003</b>	<b>C-1</b>
	<b>Appendix D: Paper published in the conference proceedings of the 10<sup>th</sup> International Conference on Information Systems Analysis and Synthesis, June 2004</b>	<b>D-1</b>
	<b>Appendix E: Article submitted for publication in Computers &amp; Security, May 2006</b>	<b>E-1</b>

## List of Figures

Figure 1.1: Thesis layout.....	13
Figure 3.1: The different development waves of Information Security.....	36
Figure 3.2: Common Body of Knowledge for Information Security suited to industry .....	52
Figure 4.1: IT authority levels .....	61
Figure 4.2: Information Security responsibilities of IT authority levels .....	67
Figure 6.1: The Information Security community – Scope of the ISRA model.....	84
Figure 6.2: The scope of the Common Body of Knowledge for Information Security suited to industry.....	85
Figure 6.3: Conceptual view of the ISRA model.....	87
Figure 7.1: Graphical view of the ISRA Dimensions .....	92
Figure 7.2: y-slicing.....	94
Figure 7.3: The Board Briefing Document on IT Governance.....	96
Figure 7.4: The Commonwealth Protective Security Manual .....	97
Figure 7.5: The Financial Issues of Corporate Governance report (Cadbury Report).98	
Figure 7.6: The Governance, Control and Audit for Information and Related Technology (COBIT) document.....	99
Figure 7.7: The Information Security Governance: Guidance for Boards of Directors and Executive Management document .....	100
Figure 7.8: The Information Technology - Guidelines for Management of IT Security (GMITS) document.....	101
Figure 7.9: The International Organization for Standardization (ISO 17799).....	102
Figure 7.10: The IT Infrastructure Library on Security Management document .....	103
Figure 7.11: The KING report .....	104
Figure 7.12: The National Institute of Standards (NIST) handbook .....	105
Figure 7.13: z-slicing .....	106
Figure 7.14: Board level .....	109
Figure 7.15: Executive Management level .....	110
Figure 7.16: Middle Management level.....	111
Figure 7.17: Technical Management level.....	112
Figure 7.18: Information Security Management level.....	113

Figure 7.19: User level.....	114
Figure 7.20: Results of the zx-slicing method .....	116
Figure 7.21: Results of the yx-slicing method.....	117
Figure 8.1: Scope of prototype.....	124
Figure 8.2: Organisational structure of Bekker & du Toit Optometrists .....	125
Figure 8.3: Login screen .....	127
Figure 8.4: Home screen for Board level.....	128
Figure 8.5: Information Security Awareness Program screen.....	129
Figure 8.6: Detailed information on computer ethics .....	130
Figure 8.7: Detailed information on corporate governance (including Information Security governance) .....	131
Figure 8.8: Detailed information on physical security.....	132
Figure 8.9: Detailed information on security policy .....	133
Figure 8.10: Information Security awareness test for computer ethics .....	135
Figure 8.11: Information Security awareness test for corporate governance .....	137
Figure 8.12: Information Security awareness test for physical security .....	139
Figure 8.13: Information Security awareness test for security policy .....	141
Figure 8.14: Results for tests taken.....	142
Figure 8.15: Home screen for Executive Management level.....	142
Figure 8.16: Information Security Awareness Program screen.....	143
Figure 8.17: Detailed information on computer ethics .....	144
Figure 8.18: Detailed information on corporate governance (including Information Security governance) .....	145
Figure 8.19: Detailed information on physical security.....	146
Figure 8.20: Detailed information on security policy .....	147
Figure 8.21: Information Security awareness test for computer ethics .....	149
Figure 8.22: Information Security awareness test for corporate governance .....	151
Figure 8.23: Information Security awareness test for physical security .....	153
Figure 8.24: Information Security awareness test for security policy .....	155
Figure 8.25: Results for test taken .....	156
Figure 8.26: Home screen for User level.....	156
Figure 8.27: Information Security Awareness Program screen.....	157
Figure 8.28: Detailed information on computer ethics .....	158
Figure 8.29: Detailed information on physical security.....	158

Figure 8.30: Detailed information on security policy .....	159
Figure 8.31: Information Security awareness test for computer ethics completed by the secretary .....	161
Figure 8.32: Information Security awareness test for physical security completed by the secretary .....	163
Figure 8.33: Information Security awareness test for security policy completed by the secretary .....	165
Figure 8.34: Results for tests taken by the secretary .....	166
Figure 8.35: Information Security awareness test for computer ethics completed by the accountant .....	168
Figure 8.36: Information Security awareness test for physical security completed by the accountant .....	170
Figure 8.37: Information Security awareness test for security policy completed by the accountant .....	172
Figure 8.38: Results for tests taken by accountant .....	173
Figure 8.39: Reports option .....	174
Figure 8.40: Selecting the IT authority level for the report .....	174
Figure 8.41: Selecting Information Security issues for the report .....	175
Figure 8.42: Report requested .....	176
Figure 8.43: Information Security retrieval option .....	178
Figure 8.44: Selecting an Information Security issue for retrieval process .....	178
Figure 8.45: Selecting one or more Information Security documents .....	179
Figure 8.46: Results of retrieval process .....	180

# **Chapter 1**

## **Introduction**



## **1.1 Introduction**

In today's competitive business environment, information is the lifeline of many organisations (Broderick, 2001; Finne, 2000; Posthumus & Von Solms, 2004; Squara, 2000; Streff & Zhou, 2006; Von Solms & Von Solms, 2005). Information is therefore a valuable resource and should be protected and secured accordingly. If, for any reason, valuable information is compromised, the organisation could lose time, manpower, money and/or business opportunities (Deloitte, Touche & Tohmatsu, 2005; Dhillon & Moores, 2001; Whiteman & Mattord, 2003). This can even lead to damage to the organisation's reputation, or worse, the disintegration of the organisation itself.

According to the 2005 survey on Information Security breaches, malicious software (such as viruses and worms) have never been as big a security threat as they are today (PriceWaterhouseCoopers & Dti, 2005). An example of such malicious software is the MyDoom worm. The MyDoom worm was first detected on 26 January 2004 and it quickly spread across the Internet, rapidly congesting e-mail servers by spreading millions of infected messages (Becker, 2004; Roberts, 2004). The following are some of the incidents for which MyDoom was responsible:

- MyDoom attacked and took down SCO.com (an online technology company) and as a result took the domain off-line for five weeks.
- My Doom attacked and took down a recording company in the USA (RIAA.com).
- MyDoom used the Google Search Engine to search for e-mail addresses and took down Google for hours.

The MyDoom worm has been one of the largest e-mail incidents in computer history (F-Secure, 2004). The damage that MyDoom caused is estimated to be in the region of \$40 billion worldwide (Information Week, 2004). Security companies interrupted more than 3.4 million copies of MyDoom. This means one in 12 e-mails were infected (Becker, 2004).

MyDoom was only one of many Information Security threats that caused havoc all over the world. The serious consequences of such threats underline the necessity for Information Security to be properly managed in order to ensure that Information Security

breaches are restricted to a minimum (Andersen, 2001; Moulton & Coles, 2003; Von Solms & Eloff, 2004; Williams, 2001).

## **1.2 Motivation for this study**

Managing Information Security among employees in any organisation is a daunting task and easier said than done. Human-related Information Security breaches within organisations (such as exposing passwords to unauthorised people) are primarily caused by employees who have not been made aware of the importance of protecting the information they work with. If employees are not properly made aware of Information Security issues, they could not be held accountable if the information is compromised. *All employees in an organisation should therefore be made aware of their role and responsibility towards securing the information they work with.* This realisation provided the primary motivation for this study, while it was also prompted by the additional insights discussed below.

### **1.2.1 Information is the lifeline of many organisations and must be protected**

We live in an era in which information is becoming increasingly valuable and the organisation with the best information on which to base management decisions will be the likeliest to win and prosper (Finne, 2000). It is therefore essential to secure information properly against all possible Information Security threats (from inside as well as outside the organisation). The following examples explicitly show the consequences of failing to do so:

- The Sasser Worm was first detected on 30 April 2004. It spread rapidly and infected more than a million Windows machines worldwide, using a security hole in the Windows operating system (Roberts, 2004). Microsoft offered a reward of \$250 000 for the apprehension of the culprit. Train traffic was halted in Australia (Rail Infrastructure Corporation - RailCorp), leaving 300 000 travellers stranded, while two country hospitals in Sweden were infected and left with 5 000 computers and X-ray equipment off-line (F-Secure, 2004). Sasser affected the *availability* of information, which led to the compromising of services such as those provided by RailCorp.

- According to the Donau University Krems, an Italian couple hacked into the security system of two American banks and stole credit card data pertaining to nearly 1 500 clients. They used the credit cards for various purchases. In one month, they purchased \$750 000 worth of lotto tickets and the winnings of \$400 000 were transferred directly into their bank account (Fotinger & Ziegler, 2004).
- According to the CSI/FBI Computer Crime and Security Survey, the 639 organisations that participated in the survey suffered a total loss due to *unauthorised use of computers* for 2005 of \$130 104 542 (CSI/FBI, 2005).
- In 2002 a University in Minnesota revealed sensitive information to 400 donors, exposing the recipients who had received their kidneys (Sullivan, 2002). According to John Halamka, the chairman of the New England Health Electronic Data Interchange Network, such inadvertent information Security incidents are a result of the fact that the healthcare environment spends a mere 2% to 3% on their IT budget, as opposed to other industries that spend up to 12% (Hoffman, 2006).

These are but a few examples indicating the serious consequences resulting from Information Security breaches.

### **1.2.2 Information Security is a human-related issue**

Many Information Security breaches that occur within organisations are linked directly to human-related issues, such as downloading unauthorised software from the Internet (CompTIA, 2006; CSI/FBI, 2005; Deloitte, Touche & Tohmatsu, 2005; Pratt, 2006). Employees could be seen as an Information Security vulnerability if they do not possess the necessary skills and knowledge to protect the information they work with (Streff & Zhou, 2006; Whiteman, 2004). Furthermore, insider Information Security threats occur far more frequently than threats from outside (Deloitte, Touche & Tohmatsu, 2005). Information Security therefore clearly has a human-related side and should not be treated as a technical issue only (Hone & Eloff, 2002; Von Solms & Von Solms, 2004b). Even though the human-related issues have been recognised as playing a pivotal role in Information Security, they have not yet received sufficient attention (CSI/FBI, 2005; Siponen, 2000a).

### **1.2.3 Lack of Information Security awareness**

Organisations should ensure that their employees are aware of all the existing Information Security rules and regulations (including relevant national and international law), to enable them to incorporate such rules and regulations into daily routine when working with information (Berinato, 2005; CompTIA, 2006; Lewis, 2000; Nosworthy, 2000; Pratt, 2006). These rules and regulations are combined in an Information Security policy document that is used as a basis for all other Information Security subpolicies, procedures and standards (Von Solms & Von Solms, 2004a). There is a lack of properly defined Information Security policies globally (Von Solms, 2005a). During 2004 in the UK, for example, only a third of businesses had formally defined Information Security policies in place (PriceWaterhouseCoopers, 2004). The absence of such policies directly contributes to the lack of Information Security awareness within an organisation. If employees are not aware of how to protect information, such information becomes vulnerable and open to attack.

Global statistics show that although many organisations believe that Information Security awareness is important, not enough is currently being invested in it (CSI/FBI, 2005). Even if there are Information Security awareness programmes in place, they are very often neither implemented nor enforced. Statistics show that only 6% of organisations present any Information Security awareness programme to their newly appointed employees (Deloitte, Touche & Tohmatsu, 2005). Statistics also show that 35% of global organisations do not make their employees aware of any possible Information Security threats (Deloitte, Touche & Tohmatsu, 2005). This lack of Information Security awareness could lead to information being compromised.

### **1.2.4 Lack of Information Security governance**

Corporate governance is the system or method by which companies are directed, controlled and managed (Cadbury Report, 1992). The ultimate responsibility for corporate governance lays with top management, for instance the Board and Executive Management (Von Solms, 2005a). Top management should therefore ensure that all resources within the organisation are managed at all times. One subset of corporate governance is Information Security governance – which addresses the protection of information. Top management is therefore also responsible for protecting information.

Although Information Security governance is addressed by top management, this effort is still not enough (Kwok & Longley, 1999). Only 20% of organisations view Information Security as a priority to be addressed at the Chief Executive Officer (CEO) level, while 42% of top management still believe that Information Security is an IT function (Berinato, 2005; Ernest & Young, 2004). This shows a clear lack of Information Security governance. Employees are not going to adhere to Information Security policies if top management does not get involved (Ernest & Young, 2003).

### **1.2.5 Monitoring the enforcement of Information Security**

It is no use having Information Security policies if it is not possible to monitor and enforce compliance with such policies (Von Solms & Von Solms, 2004a). This monitoring must occur on a regular basis to ensure ongoing Information Security – it is not a one-time investment (Danchev, 2003; Ernest & Young, 2004). Why implement Information Security controls if you cannot determine whether or not they are successful? For example, it is totally unacceptable for an organisation to find, six to 12 months after an employee has left the organisation, that this employee still has access to organisation-related information! The only way to stop such unauthorised use of information is through regular monitoring of Information Security.

## **1.3 Problem statement**

Many organisations have a misguided sense of how difficult it is to secure their information and many of them want a “quick-fix tool” to ensure it (Cutler, 2000; Deloitte, Touche & Tohmatsu, 2005). Organisations should understand that there are no quick-fixes in Information Security and that a proper Information Security culture must be cultivated within the organisation (Gallivan & Srite, 2005; Von Solms & Von Solms, 2005). This Information Security culture should ensure that all employees are aware of how to properly protect information within the organisation.

Information Security awareness is about ensuring that all employees in an organisation are made aware of their role in and responsibility for securing the information with which they work. Employees cannot be held accountable for loss of or damage to information if they have not been made aware of how to properly secure the information with which they work. Thus, there is a growing urgency about identifying all employees and their

role (s) in an organisation and ensuring that they are aware of their responsibilities as far as Information Security is concerned.

This research recognises the following needs within the Information Security environment.

- *There is a need to enhance Information Security awareness among all employees* – from Information Security professionals to employees with no or little Information Security knowledge or experience. While in some cases Information Security policies are available and enforced by Information Security professionals, in many other cases employees have no proper Information Security background or knowledge to protect information within the organisation (Cutler, 2000; Deloitte, Touche & Tohmatsu, 2005; Streff & Zhou, 2006; Whiteman, 2004). Employees are consequently still considered to constitute one of the primary Information Security threats (CSI/FBI, 2005).
- Information Security is not a purely technical issue, but it is often treated that way (Leach, 2003; Posthumus & Von Solms, 2004; Von Solms & Von Solms, 2005; Wood, 2004). Currently there is no balance between technical and non-technical, human-related Information Security issues. The technical Information Security issues still overshadow the non-technical, human-related Information Security issues. *Organisations should recognise and treat Information Security as both a technical and a non-technical, human-related issue.*
- *There is a need to ensure that employees are not burdened with unnecessary information regarding Information Security* that is not relevant to their specific working environment (National Institute of Standards and Technology, 2000). Employees should be exposed only to those Information Security issues related to their Information Security responsibilities. This will ensure that employees do not waste their time and effort on irrelevant information.

This thesis is aimed mainly at making a contribution towards *enhancing Information Security awareness in industry*. A three-dimensional Information Security Retrieval and Awareness (ISRA) model will be proposed, which adopts a fresh approach towards enhancing the Information Security awareness of all employees in an organisation. The

principal issues to be addressed in this thesis so as to achieve this goal can be defined in the form of the four research questions below.

### **1.3.1 What is the current status of Information Security awareness?**

Information Security is constantly developing to keep up with new technologies, since the latter lead to new Information Security risks and threats. The Information Security environment should be acutely aware of these risks and threats and of how to prevent or minimise them. This research question calls for investigating the Information Security sectors in the Information Security environment, in order to determine the current Information Security awareness status of each sector.

### **1.3.2 What is meant by non-technical, human-related Information Security issues?**

Information Security comprises both technical and non-technical, human-related Information Security issues. Research primarily focuses on the technical issues, such as firewalls and encryption, while the non-technical, human-related Information Security issues receive far less attention (Pfleeger, 1997; Von Solms & Eloff, 2004). This research question calls for an investigation into the non-technical, human-related Information Security issues. It is important to understand what is meant by non-technical, human-related Information Security issues if one is to ensure that they receive the same attention as the technical Information Security issues.

### **1.3.3 What Information Security issues should employees be aware of to enhance Information Security awareness?**

There are currently a large number of documents available, each addressing the management and implementation of various Information Security issues. The Information Security environment aims to group these Information Security issues together to form a Common Body of Knowledge for Information Security. This Common Body of Knowledge will be used primarily as guidelines for employees on how to secure the information they work with. Although no universally accepted Common Body of Knowledge for Information Security exists yet, efforts are being continued to establish one (Crowley, 2003; Wilson & Hash, 2005).

State-of-the-art Information Security documents should be used to create such a Common Body of Knowledge for organisations to enhance Information Security awareness among their employees. This research question calls for the identification and investigation of state-of-the-art Information Security documents with a view to proposing a Common Body of Knowledge for Information Security suited to industry.

### **1.3.4 How can one prevent employees from being burdened with unnecessary information?**

A Common Body of Knowledge for Information Security suited to industry will comprise a huge amount of information regarding the management and implementation of Information Security. However, *all* the employees need not be aware of *all* the Information Security issues. Therefore – how can a Common Body of Knowledge for Information Security be structured to simplify the process of identifying Information Security issues relevant to a specific employee? This research question calls for the presentation of a Common Body of Knowledge for Information Security suited to industry and proposes a method for creating groups of employees with the same Information Security responsibilities. The aim of such grouping is to further simplify the process of identifying the Information Security issues relevant to a specific employee, and to ensure that employees are not weighed down with unnecessary information.

## **1.4 Terminology used in this thesis**

It is important to understand the key terms used in this study. Detailed terminology and concepts will be explained where appropriate within the thesis. This section provides an overview of the key terms that are used throughout the thesis only.

### **1.4.1 Information Security**

The International Organization for Standardization (ISO) is a global organisation that has about 110 countries as members. ISO has compiled an original document (ISO7498/2) that defines Information Security in terms of five services (Pfleeger, 1997; Von Solms & Eloff, 2004). The ISO 7498/2 is considered one of the best reference frameworks for introducing Information Security (Doherty & Fulford, 2006; Von Solms, 1999; Von Solms, 2005a). The five services that ISO identifies are *identification and*



*authentication; authorisation; confidentiality; integrity; non-repudiation* (Pfleeger, 1997; Von Solms & Eloff, 2004). Each of these services will be defined below.

### **1.4.1.1 Identification and authentication**

The first service, **identification and authentication**, is put in place to ensure that only authorised parties are able to gain access to a system (or part of a system). The first part of this service is about determining whether or not a party who is trying to gain access to a system, is cleared for access. This process is called “identification”. The party presents a user ID to be identified. Once identified, the system should also make sure that the party is who it/he/she claims to be. This process is called “authentication”. Such an authentication process occurs by means of something the party knows, such as passwords, or something the party has, such as an access token, or something the party is, such as fingerprints (Von Solms & Eloff, 2004).

### **1.4.1.2 Authorisation**

The next step towards enforcing Information Security is **authorisation**. This involves determining whether or not the authenticated party has the right to access the information in question (Von Solms & Eloff, 2004). The authorisation process can for example, involve the use of an access control list that contains records of all authenticated parties and their access rights to specific information (Pfleeger, 2003). By making use of such a list, the system ensures that only authorised users gain access to specified information.

### **1.4.1.3 Confidentiality**

The third service, **confidentiality**, is an Information Security characteristic as well as a service and is put in place to protect information from unauthorised access. The purpose of confidentiality is to ensure that information is not disclosed to any unauthorised party (International Federation of Accountants, 2000).

### **1.4.1.4 Integrity**

The purpose of the fourth service, **integrity**, is to ensure that information is still in its original form and that no tampering or alteration has taken place. In other words, only authorised parties may change the content of information and unauthorised modification must be prevented.

#### **1.4.1.5 Non-repudiation**

The last step towards enforcing Information Security is **non-repudiation** or **non-denial**. This service ensures that no action that was taken and that affects Information Security, can be denied at a later stage (Von Solms & Eloff, 2004). For example, the non-repudiation process uses digital signatures (an electronic protocol that attempts, but in an incomplete way, to produce the same effect as a real signature) to provide a party that sends information the option to digitally sign a document to verify that he/she sent it. A digital signature is therefore a mark that only the sender can make, but can easily be recognised as belonging to the sender (Pfleeger, 2003).

#### **1.4.2 Availability of information**

Availability of information means that such information is accessible to *authorised* parties at any time (International Federation of Accountants, 2000).

#### **1.4.3 Information Security awareness**

Information Security awareness entails ensuring that all stakeholders in an organisation understand their role and responsibility towards securing the information they work with. They should be aware of Information Security threats and how to successfully prevent them from happening (National Institute of Standards and Technology, 2000).

#### **1.4.4 Information Security controls**

Information Security controls are the security processes and procedures implemented to minimise or prevent the occurrence of any possible threats to information (Whiteman & Mattord, 2003).

#### **1.4.5 Information Security governance**

Corporate governance is the system or method by which companies are directed, controlled and managed (Cadbury Report, 1992). The accountability for corporate governance ultimately rests with top management (Von Solms, 2001b). A subset of corporate governance is Information Security governance – which is aimed at protecting information. Top management is therefore not only accountable for the status of Information Security in an organisation, but also responsible to ensure that Information Security is implemented and managed within the organisation.

### **1.4.6 Information Security management**

Information Security management is about maintaining Information Security in an organisation (Pfleeger, 1997). For the purpose of this thesis, Information Security management is about ensuring the identification and authentication, authorisation, confidentiality, integrity and non-repudiation of information, through proactive management and understanding the risks, threats and vulnerabilities involved.

### **1.4.7 Information Security plan**

An Information Security plan identifies and organises the security activities within an organisation (Pfleeger, 2003). According to Pfleeger, an Information Security plan should include issues such as an Information Security policy, Information Security requirements, recommended controls and implementation (Pfleeger, 2003). An Information Security plan should also consist of strategic, managerial and technical Information Security issues (Von Solms & Eloff, 2004). Each of these Information Security issues should be planned, implemented and managed properly, as well as be complied with.

### **1.4.8 Information Security policies**

An Information Security policy is a set of documentation that contains Information Security rules and regulations (National Institute of Standards and Technology, 2000). These security rules and regulations may include the implementation and management of hardware, software and information. One purpose of an Information Security policy is to indicate how to protect the organisation's information assets from all security threats. It is important that all organisations ensure that they have an Information Security policy in place to ensure that all information is correctly and fully secured.

### **1.4.9 Threats**

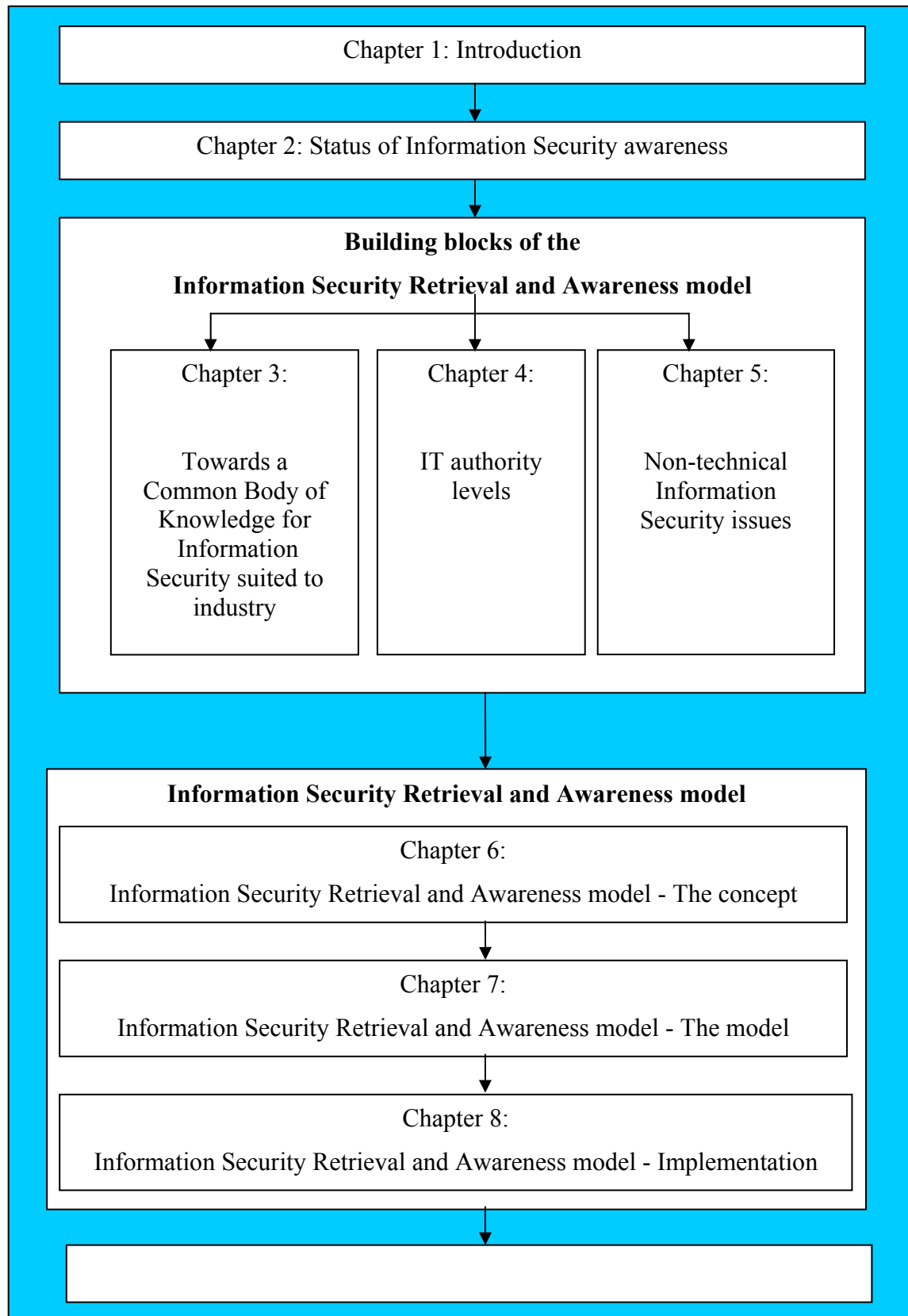
Threats are acts (accidental or intentional) that can inflict various types of damage to information, compromising the identification and authentication, authorisation, confidentiality, integrity or non-repudiation of information and ultimately resulting in significant losses (National Institute of Standards and Technology, 2000).

### **1.4.10 Vulnerability**

Vulnerability is a weakness or fault in a system that exploits information or exposes it to possible attacks, resulting in information security threats (Whiteman & Mattord, 2003).

## 1.5 Thesis layout

Figure 1.1 graphically depicts the layout of the thesis.



*Figure 1.1: Thesis layout*

**Chapter 1** serves as an introduction to the research study by providing the motivation for the study and by defining the problem statement and issues to be addressed in it. In addition, this chapter provides an explanation of the key terms used throughout the thesis. The chapter concludes with an overview of the remaining chapters.

In **Chapter 2** the status of Information Security awareness is investigated within the Information Security environment. The latter is divided into three sectors (i.e. government, industry and academia). The Information Security awareness status of each sector is investigated next. The chapter concludes by recognising that there is still a serious need for enhancing Information Security awareness in all of these sectors. For the purpose of this thesis, the focus will be on enhancing Information Security awareness in the *industry sector*.

The next chapter, **Chapter 3**, provides a perspective on the ongoing development of Information Security over the last few years. The different development stages (waves) of Information Security are identified and explained in the light of the growing need for Information Security awareness in the Information Security environment. Additionally, Chapter 3 provides an overview of current state-of-the-art Information Security documents and reveals that these documents contain large amounts of information on how to protect information. The documents are used regularly by industry to group together information regarding the management and implementation of Information Security and thus to form a Common Body of Knowledge for Information Security. Chapter 3 concludes by proposing such a Body of Knowledge suited to industry that will address the limitations of current Common Bodies of Knowledge within this domain.

**Chapter 4** is devoted to grouping stakeholders in industry into different IT authority levels. The purpose of such grouping is to determine the specific Information Security issues from the proposed Common Body of Knowledge for Information Security suited to industry that each group should be made aware of. Different ways of grouping stakeholders into IT authority levels are explored. Each IT authority level will be assigned specific roles and responsibilities in respect of securing the information they work with. Grouping stakeholders into IT authority levels will ensure that stakeholders are exposed only to the information regarding Information Security issues that is relevant

to their specific working environment. This will also ensure that stakeholders are not burdened with unnecessary information.

In **Chapter 5** the different *non-technical*, human-related Information Security issues that form part of the proposed Common Body of Knowledge for Information Security suited to industry are identified. This is followed by a discussion of each of these issues.

**Chapter 6** presents the reader with an overview of the proposed Information Security Retrieval and Awareness (ISRA) model. This entails a discussion of the scope of the proposed model, as well as a conceptual view thereof.

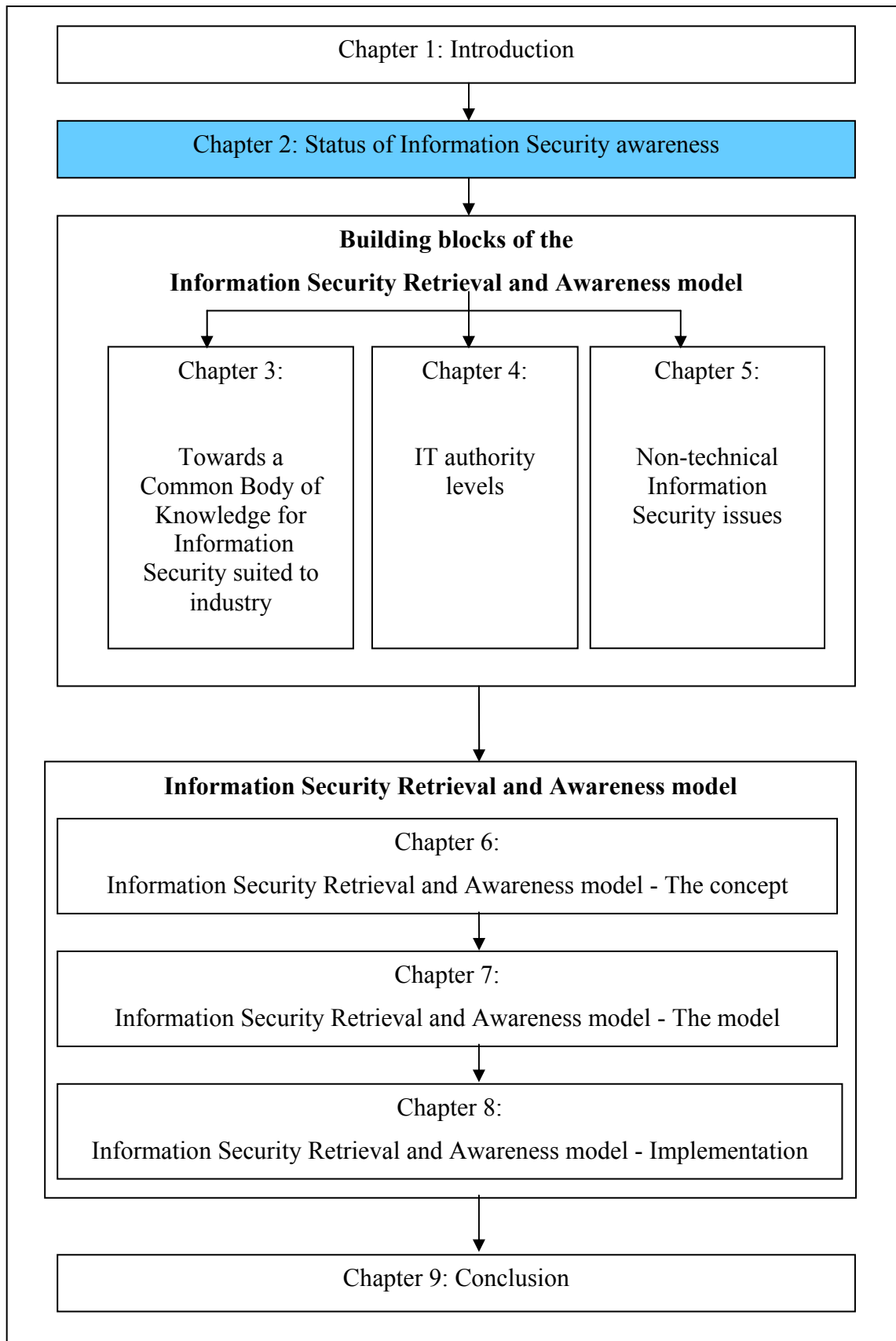
The next chapter, **Chapter 7**, is devoted to an in-depth discussion of each part of the proposed model. In this way, the three dimensions that constitute the first part of the model, namely non-technical Information Security issues, IT authority levels and Information Security documents, are discussed in detail. This is followed by detailed discussions of the second part of the proposed model – Information Security Retrieval and Awareness – as well as the third part – Measuring and Monitoring.

**Chapter 8** provides a look at the implementation of a prototype that was developed to illustrate the working of the ISRA model. The specifications of the prototype are listed in Appendix A and the user's guide is provided in Appendix B of this thesis. The prototype was implemented in a real-life industry-based organisation. This chapter proves that the ISRA model is not merely a theoretical concept, but that it can indeed be implemented successfully.

The thesis culminates in **Chapter 9**, where the author summarises the research undertaken and weighs up the pros and cons of the proposed Information Security Retrieval and Awareness model. The chapter concludes with some suggestions for future research.

## **Chapter 2**

# **Status of Information Security awareness**





## 2.1 Introduction

Since many organisations around the globe are largely dependent on their resources, these resources should be properly utilised and managed. One such a resource that is becoming more and more valuable is information. If the information within the organisation is compromised, the organisation could suffer serious consequences such as loss of income or even legal action. Information should therefore be seen as a valuable resource and should be protected to the best of the organisation's ability. This protection of information is called "Information Security". The primary goal of Information Security is to protect information by ensuring that the availability, confidentiality and integrity of information is not compromised in any way (Aljifri & Navarro, 2003; Finne, 2000; National Institute of Standards and Technology, 2000; Pfleeger, 1997; Von Solms, 1999).

Information Security is becoming an established discipline as more and more businesses realise its value. In a study by the META Group (2000) regarding the implementation of Information Security within organisations after the turn of the millennium, many Information Technology (IT) organisations named Information Security as their number one priority. This shows that the urgency of protecting information has become an important issue under discussion in the Information Security community. An important aspect that must be addressed in this regard is Information Security awareness (Deloitte, Touche & Tohmatsu, 2005; Lewis, 2000; Nosworthy, 2000; Schultz, 2004; Thomson & Von Solms, 1998; Wood, 1995).

Information Security awareness is about guaranteeing that all employees are aware of the rules and regulations regarding securing the information within the organisation (Schultz, 2004; Siponen, 2001; Thomson & Von Solms, 1998). Only if employees are made aware of their role and responsibility towards securing information can they be held accountable should the information they work with be compromised in any way. Organisations should understand that they can implement top-range technologies, but if the employees who work with those technologies are not aware of the threats involved and how to prevent them, the technologies are useless (Von Solms, 2001a). Information Security awareness should therefore form an integral part of any organisations' overall Information Security management plan. Information Security Awareness also means that organizations have

the ability to be able to specify security services and mechanisms needed and to judge the level and veracity what is being offered by vendors.

There are three different Information Security sectors within the Information Security community that address Information Security awareness in some way or another (Crowley, 2003; Hillburn, 1999). These three sectors are **government**, **industry** and **academia** (Bishop, 2000b; Crowley, 2003; Hillburn, 1999; The White House, 2000; Yasubsac, 2002). Each sector has a different role to play to ensure proper Information Security awareness within the broader Information Security community. The Information Security management plan will thus be different for every separate Information Security sector depending on its individual needs.

The purpose of this chapter is to investigate the current state of Information Security awareness. The remainder of this chapter will therefore be devoted to a discussion of the state of Information Security awareness within each of the three Information Security sectors, i.e. the government, industry and academic sectors within the Information Security community.

## **2.2 The state of Information Security awareness in the government sector**

The first sector within the Information Security community that addresses Information Security awareness is the government sector (Crowley, 2003; Streff & Zhou, 2006; Yngstrom & Bjorck, 2004). This sector consists of government departments that attend to Information Security for the benefit of a specific country and that receive government funds.

The government sector addresses Information Security awareness by aiming to ensure that all information users (from individuals to organisations) are made thoroughly aware of all Information Security laws and regulations on how to protect information properly. This includes the legal consequences should the availability, integrity or confidentiality of a user's (organisation's or even the country's) information be compromised.

Ensuring the availability, integrity and confidentiality of information has become a daunting task owing to the growing development of new and better technologies. These new and better technologies have pushed the global society into the Digital Age, where computers and networks are the order of the day and where new threats against people, information and their technologies have subsequently emerged (Fisher, 2001). People trust this digital environment without realising that computers and networks are vulnerable and without proper protection, open to attack (Sullivan, 2005). There is clearly a dire need for all users to be made properly aware of all possible information security threats and to ensure (to the best of their ability) that sensitive information (such as in the healthcare and banking professions) is protected against harmful attacks. This task falls squarely on the shoulders of the government sector.

### **2.2.1 Current Information Security awareness initiatives within the government sector**

A great deal of research has been conducted by numerous experts and professionals to enhance Information Security awareness in the government sector (Andersen, 2001; Bishop, 2000a; Fisher, 2001; Minihan, 1998; Ngo & Zhou, 2005; Yasubsac, 2002). This research has been around for many years, but because of the on-going development of new technologies (and as a result new risks) it is still considered very relevant and an important issue that should be addressed by governments around the globe (Ngo & Zhou, 2005).

Many countries (such as the United States of America (USA), Germany and South Africa) have realised the grave importance of putting Information Security protection laws and standards in place to ensure that the information within their country is protected at all cost. The government sector has responded to this need by defining directives to enhance overall Information Security awareness and by sensitising people to the importance of securing and protecting information (Bogolea & Wijekumar, 2004).

Countries such as the USA started addressing the need for enhanced Information Security awareness quite some time ago. The USA government created institutions such as the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to enhance the overall Information Security situation within their country. NIST,

formally known as National Bureau of Standards (NBS), was established in 1901 as a federal agency within the USA. Its primary aim was to “develop and promote measurement, standards and technology to enhance productivity, facilitate trade and improve the quality of life” (National Institute of Standards and Technology, 2000). The Information Technology Security and Networking (ITSN) division is a subdivision of NIST and addresses more recent security issues identified by NIST (National Institute of Standards and Technology, 2000). The USA government encourages the ITSN division to establish, implement and test information security policies, procedure and technologies for the scientific community. In addition, the National Security Agency (NSA) was created in November 1952 to secure all sensitive and classified information resources within the USA. NSA understands that it is important to ensure the continuous development of their most important resource, namely their employees. The agency therefore established the Associate Directorate for Education and Training (ADET), which is responsible for developing, delivering and maintaining learning development opportunities and solutions for the workforce (National Security Agency, 2006).

A further initiative to enhance Information Security Awareness in the government sector in the USA, is the National Colloquium for Information Systems Security Education (NCISSE). This colloquium was founded in 1996 and aims to become the leading supporter for implementing courses of instruction in information security in education (NCISSE, 2006). Its Australian affiliate is CISSE-AP. The AP is an abbreviation for Asia-Pacific (CISSE-AP, 2006).

Germany is another example of a country in which the government started to address Information Security awareness quite some time ago. Germany established special task forces for the securing of information as early as 1986 and in 1990 the Federal Office for Information Security (“Das Bundesamt für Sicherheit in der Informationstechni” - BSI) was established. This task force is the central IT security service provider for the German government. BSI conducts research within the area of IT security to enhance the security of German society at large. The services and research results BSI delivers are aimed at the users and manufacturers of information technology products (BSI, 2002). The Germany government promotes IT security inside Germany so that everyone can make the most of the opportunities opened up by the information society.

Another country that has recently realised the urgency of and need for Information Security awareness is South Africa. The South African government introduced the Electronic Communications and Transactions (ECT) Act in 2002, which addresses important Information Security issues such as customer protection and the protection of critical databases (South African Government, 2002). This means that all organisations can be held accountable if client information is compromised due to improper protection. This act forces all organisations to realise the importance of Information Security and to ensure that all their employees are aware of all relevant Information Security issues.

The examples mentioned above illustrate that Information Security awareness has been on the working agenda of some governments for a long time, while others have only recently realised the importance of Information Security. Governments should realise that technology is continuously developing and that Information Security should keep up with these developments. They should therefore ensure that their initiatives regarding Information Security awareness are continuously updated and renewed.

### **2.3 The state of Information Security awareness within the industry sector**

Industry is identified as the second sector within the Information Security community that attends to Information Security awareness. This sector consists of business ventures that vary in size, wealth and business goals. The main purpose of Information Security awareness within the industry sector is to ensure that all stakeholders are aware of all the rules and regulations aimed at securing the information they work with. All stakeholders should also understand that industry in general is heavily dependent on information as well as on the technology that protects it (Furnell, Gennatou & Dowland, 2002; Zhu, Xu & Kraemer, 2006). If the availability, integrity or confidentiality of information is compromised in any way, the organisation can experience business disruptions, direct financial losses, damage to its reputation, loss of data, etc. (PriceWaterhouseCoopers, 2004). There is thus a critical need to ensure that all users of information are made properly aware of how valuable information is, and what the consequences are if they do not accurately secure the information with which they work.

### **2.3.1 Issues to be addressed when aiming to enhance Information Security awareness in industry**

A number of prominent Information Security issues need to be addressed when aiming to enhance Information Security awareness in industry (Anderson, 2003; Deloitte, Touche & Tohmatsu, 2005; Hansche, 2001; Lewis, 2003; Morwood, 1998; Siponen, 2000a; Spurling, 1995; Von Solms & Von Solms, 2005).

#### **2.3.1.1 Information Security is a human issue**

Organisations should realise that the Information Security profile for employees has changed over the past few years. The employee profile has changed from one where all employees were Information Security specialists to one where many employees are barely computer literate (Thomson & Von Solms, 1998). The consequent lack of Information Security awareness has led to a need in industry for all employees to be made aware of all relevant Information Security policies within the organisation (Crowley, 2003; Danchev, 2003; Furnell, Gennatou & Dowland, 2002; Hansche, 2001; Johnson, 2000; Martins & Eloff, 2001; McCoy & Fowler, 2004; Siponen, 2001; Von Solms & Von Solms, 2004b; Wright, 1998). In spite of this realisation, a survey conducted by Deloitte, Touche and Tohmatsu (2005) shows that 45% of organisations still have not taught their employees how to identify and report Information Security incidents. It therefore remains a priority that all organisations should not only say that they take Information Security awareness seriously, but also implement it throughout the organisation.

On the other hand, even if the best technologies are implemented to protect information within organisations, the information remains at risk unless the employees use these technologies properly (Bauknight, 2005; Morwood, 1998; Von Solms, 2001a). Information Security is both a technical issue and a human-related issue (Peltier, 2005; Rostern, 2005; Thomson & Von Solms, 2005; Von Solms & Von Solms, 2004b; Waint, 2005). Statistics show that about 35% of damaging Information Security incidents originated from inside the organisation (CIO & PriceWaterhouseCoopers, 2005; Deloitte, Touche & Tohmatsu, 2005).

### **2.3.1.2 Employees should not be burdened with unnecessary information**

When employees participate in an Information Security awareness exercise, they are often saddled with unnecessary information. In other words, they are made aware of Information Security issues that are not relevant to their specific job. It is unreasonable to expect that employees should be aware of *all* Information Security issues (Irvine, Chin & Frincke, 1998). For example, an end user does not have to know how to configure and maintain a firewall – this is the responsibility of the Information Security officers. It is however essential that employees with different job responsibilities are grouped together and that those Information Security issues relevant to their specific job are identified (Kisin, 1996; National Institute of Standards and Technology, 2000; Peltier, 2005; Siponen, 2001; Thomson, 1999; Whiteman & Mattord, 2003). Employees should also be provided with the facility to request information related to Information Security that will help them in their decision-making processes.

### **2.3.1.3 The Board of Directors and Executive Management are ultimately responsible for Information Security awareness**

The responsibility for Information Security awareness lies with the Board of Directors and Executive Management (Andersen, 2001; Clarke, 1998; Deloitte, Touche & Tohmatsu, 2005; Moulton & Coles, 2003; Posthumus & Von Solms, 2004; Thomson & Von Solms, 2005; Turnbull, 2003; Vinten, 2000; Von Solms, 2001b; Williams, 2001). However, one very often finds in organisations that the Board of Directors and Executive Management lack a commitment to Information Security awareness, because they do not understand the risks involved in protecting information (Andersen, 2001). This can be the result of lack of time in an already burdened schedule, or just plain ignorance on the part of the Board of Directors and Executive Management. They should be made to understand why Information Security is needed, how it will benefit the organisation and what the consequences will be if Information Security is not taken seriously. Only if the Board of Directors and Executive Management show their commitment to Information Security will employees also start to take it seriously (Kritzinger & Von Solms, 2004).

This commitment obviously involves a financial contribution towards Information Security awareness within the organisation. Many managers in organisations tend to slash the budget to a minimum when it comes to Information Security issues (Danchev, 2003;

Furnell, Gennatou & Dowland, 2002). This clearly results from a lack of knowledge about Information Security and the benefits thereof. A further problem arises from the fact that the implementation and sustainable maintenance of Information Security awareness among stakeholders requires an on-going commitment (Nosworthy, 2000). It is the responsibility of the Board of Directors and Executive Management to ensure that sufficient funds are made available to implement a proper Information Security awareness programme.

### **2.3.1.4 Goal and content of an Information Security awareness programme**

Before an organisation can design and implement an Information Security awareness programme, one or more goals should be identified (Hansche, 2001; McCoy & Fowler, 2004; Siponen, 2000b). These goals will differ from one organisation to the next and may include issues such as changing the way users think and act towards securing information and measuring the information security level of all users. These goals can be used to keep the awareness programme on track or to evaluate the success of the awareness programme after a specific period of time.

Having identified the goals, the design phase of the Information Security awareness programme can commence (Hansche, 2001; McCoy & Fowler, 2004). This phase includes identifying the Information Security content (issues) that employees should be aware of. Internationally accepted Information Security documentation should be used as a basis for the content of the Information Security awareness programme to ensure that all security issues are addressed (Saint-Germain, 2005). All stakeholders should be involved (in one way or another) in an Information Security awareness programme to ensure that they grasp the consequences of failing to secure information within the organisation (Hulme, 2005; Siponen, 2001).

### **2.3.1.5 Appropriate Information Security awareness programme**

Organisations can use off-the-shelf products, their own Information Security awareness programme, or a combination of both. Especially smaller organisations do not always have the funding to buy an off-the-shelf Information Security awareness programme (Danchev, 2003; Furnell, Gennatou & Dowland, 2002). Furthermore, such programmes do not necessarily suit the structure of the organisation, which may differ in size, geographical location and technologies used. Finally, many of these programmes are



training programmes with little or no continuous follow-up awareness programmes afterwards. Organisations should therefore have an option to modify their own in-house Information Security awareness programme to suit their specific needs, organisational structure and financial budget.

Many Information Security awareness programmes are currently available and sold by vendors worldwide. These Information Security awareness programmes differ from one another in price, size, content and teaching methods. A few examples of Information Security vendors are Symantec, TechNo and NetIQ (Wager, 2005). Each organisation should, however, decide about its Information Security awareness approach based on its own goals and needs. Organizations could also decide to outsource their information security awareness to international known and widely accepted institutions such as the Information Systems Audit and Control Association (ISACA), the International Information Systems Security Certification Consortium (ISC)<sup>2</sup> and the SysAdmin, Audit, Network, Security Institute (SANS) ((ISC)<sup>2</sup>, 2006; ISACA, 2006; SANS, 2006).

### **2.3.1.6 Information Security awareness programmes should be measured and monitored**

Measuring is about establishing the extent to which the Information Security awareness programme is working within the organisation. The objects that are measured will differ from organisation to organisation and include products, systems, processes, security programme effectiveness and personal competence (Katzke, 2001). The measuring process should also be employed over time to indicate growth (positive or negative) in Information Security awareness within the organisation.

Closely related to measuring is monitoring. Monitoring is about finding out if procedures and processes that are implemented in an organisation are working as they should, and if they are being complied with. This is to ensure that the Information Security policy is properly implemented and all information is secured (Danchev, 2003; Ernest & Young, 2004). It is no use having an Information Security policy that addresses awareness if it is not possible to monitor and enforce compliance with such a policy (Kisin, 1996; Von Solms & Von Solms, 2004b). Monitoring helps organisations to identify vulnerable areas (such as new technologies) and it is subsequently essential to ensure that these areas are addressed as soon as possible by an Information Security awareness programme.

Information Security awareness programmes should also be monitored to ensure that they keep up with the rapid changes in technology. What is state-of-the-art today, may be obsolete in the near future (Williams, 2001). All employees should therefore be made aware of and kept up to date with all the latest technologies implemented in the organisation and how to use them properly. For each new technology used in the organisation, the organisation should ensure that a policy is designed and implemented among all employees who will use that technology. Information Security awareness should therefore be seen as an integral part of the overall Information Security process within an organisation.

### **2.3.1.7 Information Security awareness programmes should be presented regularly**

How often the Information Security awareness programme should be presented (time period), is still an open question and widely debated among professionals (Johnson, 2000; Lewis, 2003). This period could range from quarterly to semi-annually to annually and will differ from one organisation to the next according to its specific security needs. However, many specialists maintain that the more often this occurs, the better. Implementing an Information Security awareness programme should not be seen as a once-off action, but rather as an on-going commitment to securing information by old and new employees (Danchev, 2003). In a survey by Deloitte, Touche and Tohmatsu (2005), only 6% of the respondents attempted to enhance Information Security awareness among new employees. Information Security awareness should therefore become part of the day-to-day culture of any organisation where each stakeholder should make a long-term commitment to securing the information with which he/she works (Spurling, 1995).

## **2.4 The state of Information Security awareness in the academic sector**

The third sector of the Information Security community that addresses Information Security awareness is the academic sector. This sector consists of all tertiary institutions (such as universities, technikons and colleges) that have as their primary aim the providing of learners with specific skills and knowledge to prepare them for their future occupations in some field that includes Information Security as a primary or secondary

focus. In this sector Information Security awareness refers to ensuring that learners are aware of Information Security issues relevant to their specific field of study. The academic sector is therefore ultimately responsible for ensuring that the growing need for Information Security awareness (as demanded by the government and industrial sectors) is addressed by providing Information Security learners with the proper Information Security background, knowledge and skills (Armstrong & Jayaratna, 2002; Bessagnet *et al.*, 2005; Bishop, 2000a; Doherty & Fulford, 2006; Streff & Zhou, 2006; Williams, 2005).

### **2.4.1.1 Prominent research outcomes regarding Information Security awareness in the academic sector**

Information Security awareness within the academic sector has received much attention from researchers around the globe (Bishop & Frincke, 2005a; Irvine, Chin & Frincke, 1998; Williams, 2005; Wright, 1998). This shows that there is a realisation that Information Security awareness should receive proper attention in tertiary institutions.

### **2.4.1.2 Information Security should form part of undergraduate as well as postgraduate curricula**

One of the primary outcomes of research activities in the academic sector is that Information Security must be incorporated in the curricula of tertiary institutions (Armstrong & Jayaratna, 2002; Bishop, 2000b; Cockroft, 2002; Gritzalis, Theoharidou & Kalimeri, 2005; Schou, 2001; Slay & Lock, 2005; Yang, 1998). Although the USA's series of curricula for information security education has been available for 12 years and sets out clear parameters for appropriate tertiary education, research clearly indicates that there is still an ongoing need for well-designed Information Security courses in the academic sector (Committee on National Security Systems, 2006; Wright, 1998). While some tertiary institutions have strong courses and others have emerging courses, there are still institutions that offer no Information Security courses at all (Vaughn, Dampier & Warkentin, 2004). According to Vaughn, Dampier and Warkentin (2004), those with emerging and/or no courses constitute by far the biggest group.

It is important that Information Security should be incorporated at all levels in the curricula of tertiary institutions, i.e. undergraduate as well as postgraduate (Armstrong &

Jayaratna, 2002; Smith *et al.*, 2004; Werner, 2004). In the majority of cases where Information Security is included in the curricula of tertiary institutions, it is implemented at postgraduate level only. For example, according to a study done in South Africa two-thirds of all local Information Security courses were presented at postgraduate level at that time (Smith *et al.*, 2004). Another case study by Bogolea and Wijekumar (2004) confirms that Information Security issues are seriously lacking in the undergraduate degree programmes at the Pennsylvania State University at any time. Furthermore, in the majority of cases where Information Security is included at undergraduate level, the aim is merely to provide an overview of a wide range of Information Security topics (Bacon & Tikekar, 2003). The fundamentals of Information Security should however be covered in depth at undergraduate level, because many students are hired for Information Security positions before having completed their degrees or without having registered for postgraduate studies (Yurcik & Doss, 2001).

### **2.4.1.3 Information Security is multidisciplinary**

Information Security is relevant not only to Computer Science and Information Systems disciplines, but also to a variety of other study fields (for example Business Management). Because of its multidisciplinary nature, it is therefore no simple process to build Information Security into the curricula of tertiary institutions (Ngo & Zhou, 2005; Smith *et al.*, 2004; Wright, 1998). Information Security should also not be restricted to Computer Science and Information System courses, but rather be integrated with a variety of study fields as applicable. Examples of additional education fields in which Information Security awareness should play a role, are the legal and medical environments. An information Security curriculum should not only include a list of topics, it should also outline the overall pedagogy to be employed for example, assessment criteria and processes, learning laboratories or practical sessions. When Information Security is built into different study fields, the Information Security awareness curriculum should be designed in such a way that it is suited to the specific needs of every particular study field (Gritzalis, Theoharidou & Kalimeri, 2005; Irvine, Chin & Frincke, 1998).

### **2.4.1.4 Non-technical Information Security issues should also be addressed**

Information Security curricula should include both technical and non-technical (human-related) Information Security issues. Information Security is widely recognised as

technical as well as non-technical and should be treated that way (Bishop & Frincke, 2005b; Corporate Governance Task Force Report, 2004; Martins & Eloff, 2001; Von Solms & Von Solms, 2004b). However, the technical Information Security issues overshadow the non-technical issues. Many non-technical Information Security issues (such as legal issues and information policies) are simply not included in traditional Computer Science curricula (Bacon & Tikekar, 2003). For example, in a study done by Smith, Kritzinger, Von Solms and Oosthuizen (2004), far more technical Information Security issues than non-technical ones were presented in the majority of tertiary institutions in South Africa at that time. This situation should be rectified by aiming to strike a balance between the technical and non-technical Information Security issues addressed in tertiary curricula.

### **2.4.1.5 Shortage of Information Security educators and professionals**

The fact that the majority of tertiary institutions offer either emerging or no Information Security courses at all has caused a lack of sufficient education in Information Security. This obviously results in a shortage of people with proper Information Security skills, background and knowledge within the industrial and government sectors (Wright, 1998). Proper Information Security education should be in place to deliver Information Security professionals who are prepared for all security challenges within their professional working environment (Bacon & Tikekar, 2003; Smith *et al.*, 2004; Yang, 1998).

### **2.4.1.6 Information Security curricula should adhere to the requirements of government and industry**

Information Security curriculums should be structured in such a way that the needs identified by the industrial and government sectors are addressed. The Information Security curriculum should enable learners to educate and train their co-workers as soon as they themselves are employed (Yang, 1998). Additionally, Information Security curricula should include theory as well as practical exercises (Bishop, 2000a; Bishop & Frincke, 2005a; Bishop & Frincke, 2005b; Irvine, Chin & Frincke, 1998). In this way learners will be able to apply underlying Information Security principles to real-world scenarios in industry (Morneau, 2004). It is also important to note that research on the subject shows that the Information Security curriculum should not only be based on international best practices (such as BS 7799), but should also address the needs of industry (Bacon & Tikekar, 2003; Smith *et al.*, 2004).

#### **2.4.1.7 Information Security curricula should keep up with new developments**

Information Technology is growing at a rapid pace (Yang, 1998). The academic sector should identify new developments and ensure that Information Security issues related to these new developments are incorporated in the Information Security curricula as soon as possible. This will ensure that learners are kept up to date with new developments and trends in Information Security.

### **2.5 Conclusion**

This chapter was devoted to an investigation of the status of Information Security awareness in each of the Information Security sectors (government, industry and academia). Each of these three sectors addresses Information Security awareness in a different way and for different reasons.

The government sector addresses Information Security for the benefit of their specific countries. This sector aims to encourage organisations and their information users to protect valuable information in their working environment. Governments from all around the globe should continue to launch new initiatives or update and revise existing initiatives to enhance the Information Security awareness of specific countries.

Research conducted in the industry sector shows that although Information Security awareness is a well-known issue, it is not receiving enough attention yet. Information Security is still perceived as a technical issue and the non-technical, human-related side of Information Security is often overlooked. Greater emphasis should be placed on the non-technical, human-related Information Security issues, because human error (due to ignorance) accounts for many of the Information Security breaches within organisations. All stakeholders should participate in an Information Security awareness programme within the organisation to minimise Information Security breaches that occur as a result of a lack of awareness. Stakeholders should however be made aware only of the Information Security issues related directly to their job – they should not be saddled with unnecessary information. The responsibility to ensure that an Information Security awareness programme is properly implemented ultimately lies with the Board of Directors and Executive Management.

The academic sector is ultimately responsible for ensuring that learners are educated about Information Security issues. The government and industry sectors, in turn, encourage the academic sector to incorporate Information Security issues into their curricula so as to enhance the Information Security awareness of learners. Information Security is multidisciplinary and should therefore be integrated at undergraduate and postgraduate levels with the curricula of different study fields. Such curricula should adhere to requirements of government and industry and should continuously be revised to keep up with new developments in the field.

The current state of Information Security awareness in each of the Information Security sectors (government, industry and academia) indicates that there is still much need for enhancing Information Security awareness in all of these sectors. For the purpose of this thesis, our focus will be on enhancing Information Security awareness in the *industry sector*.

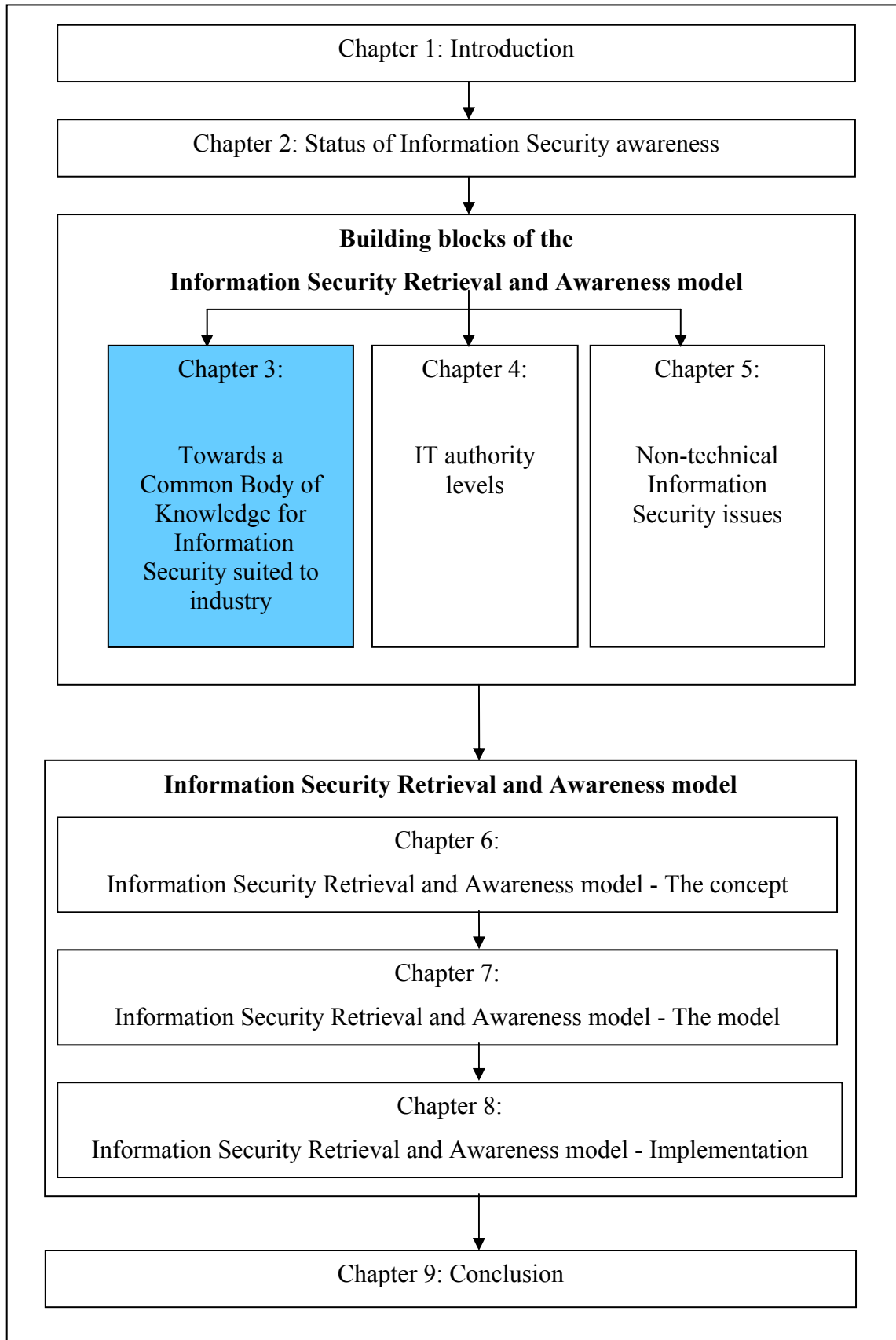
In the next chapter the development of Information Security over the past years will be investigated. In addition, various nationally and internationally accepted Information Security documents, created to keep track of these developments, will be identified and investigated. These Information Security documents contain a vast amount of knowledge regarding the implementation and management of Information Security.

## **Chapter 3**

# **Towards a Common Body of Knowledge**

**for Information Security suited to  
industry**





### **3.1 Introduction**

Information Security first emerged around the early 1950s. From then on Information Security changed and developed in many different ways. All stakeholders in an organisation should be made aware of these changes and developments to ensure that they are aware of how to secure and protect the information they work with on a day-to-day basis. This awareness can be obtained through a properly designed Information Security awareness programme. When developing such a programme, one needs to keep track of the developments in Information Security, consult different state-of-the-art Information Security documents and accordingly attempt to define a Common Body of Knowledge for Information Security (Crowley, 2003).

Chapter 3 contains a discussion of the development of Information Security and an overview of prominent nationally and internationally accepted Information Security documentation. These documents originated due to the development of Information Security and were created to keep abreast of the rapid development of Information Security. Finally, the idea of a Common Body of Knowledge for Information Security specifically suited to industry – which can be populated using these leading Information Security documents – will be introduced. The Common Body of Knowledge for Information Security proposed in this chapter will form one of the building blocks of the Information Security Retrieval and Awareness model proposed in Chapter 6.

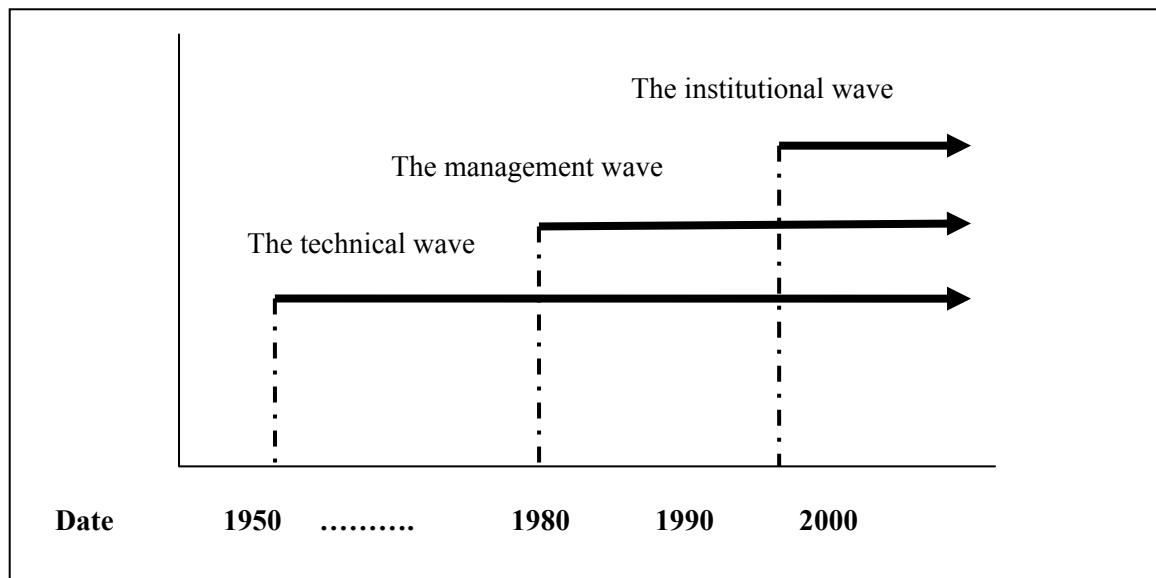
### **3.2 The on-going development of Information Security**

New technology is released on a daily basis and with each new technology come new security threats, different from those that a company is currently guarding against (Danchev, 2003). This means that each time a new technology is implemented, the security in the organisation must be updated. If this is not done, the information connected to these new technologies is open to attacks (from inside or outside the organisation). Information Security should therefore keep track with ongoing changes. These changes in Information Security can be grouped together to form paradigm shifts.

Three Information Security paradigm shifts can be identified to indicate how Information Security has developed over the past years – the technical wave (the first wave), the management wave (the second wave) and the institutional wave (the third wave) (Von

Solms, 2001a). Organisations have struggled much to keep up to date with these paradigm shifts in Information Security (Palmer, 2001).

Figure 3.1 depicts these three waves graphically on a timeline from the 1950s onwards.



*Figure 3.1: The different development waves of Information Security (Von Solms, 2001a)*

### 3.2.1 The technical wave

In the early 1950s, the security environment had a purely technical approach to Information Security (Von Solms, 2000). This technical period, during which the technical Information Security issues (such as encryption and access control lists) dominated the Information Security environment, can be identified as the “technical wave”. During this period, physical security received a great deal of attention due to the fact that data was stored and managed on centralised mainframes (Palmer, 2001). These mainframes were usually housed in a single room, where physical security such as locks and control gates were used to ensure security. The physical security in the organisation was ultimately the responsibility of the technical personnel. The rest of the employees had no responsibility towards Information Security and if anything went wrong, the technical personnel were always blamed and management had little or no influence. During this period, the centralised environment required little or no management due to the fact that information was stored in a central location that offered significant assurance that information was being kept secure.

The situation started to change in the 1960s when the “MULTICS” system (a timeshared mainframe computer system) started experiencing major security risks outside the boundaries of the physical room. This change continued with the development of extensive and cheap, yet powerful distributed systems (Palmer, 2001). Many organisations realised that there was more to Information Security than just information technology (Kisin, 1996). This realisation led to a paradigm shift from the technical wave to a more managerial way of protecting information.

### **3.2.2 The management wave**

The primary reason for the shift from the “technical wave” to the “management wave” was the shift from centralised mainframes to distributed systems. With centralised systems information security had to be assessed and managed at the human level to a high degree since all users were sharing essentially one system or a cluster of systems. Tiny computers then had the same power that mainframes had during the previous development wave. Centralised systems such as mainframes virtually collapsed as a result of cheap, distributed systems and remote computing with easy connectivity. With these new distributed systems, organisations realised that boundaries were increasingly being eroded and that organisations no longer had a hierarchical structure (Lindup, 1996). This led to technical personnel realising that management of some kind must be brought into the picture sooner or later. The management wave did not replace the technical wave, but rather enhanced and complemented it with more management input (Von Solms, 2000).

The second reason for the shift from the technical to the management wave was the increasing power of these distributed systems. A definite shift took place from dumb terminals that required little and easy security, to personal computers that needed many more security measures. For example, with a centralised system, physical security was as easy as ensuring that one locked a single room. When decentralised systems started to appear, physical security became a daunting task because all systems had to be physically secured at more than one location. This also meant that more users had access to the system – and more users increased the possibility of Information Security breaches.

The third reason for the shift to the management wave was that organisations realised that Information Security was not just a purely technical issue, but a management one as well (Von Solms, 2000). This realisation was primarily based on the concept of Information Security being also a human-related issue, requiring different management skills as opposed to purely technical ones (Lewis, 2000; National Institute of Standards and Technology, 2000; Siponen, 2000a; Whiteman & Mattord, 2003; Wood, 1995). The human being became the greatest source of computer-related loss in an organisation and therefore more time and effort had to be spent on managing non-technical, human-related issues (such as ethics and legal issues) to prevent possible Information Security breaches in the organisation (Lewis, 2000).

Towards the end of the 1990s problems with the managerial wave started cropping up. Some of the problems (or concerns) were that there were no best practices, guidelines or control measures in place to help information security managers to secure information properly. The employees in the organisation therefore did not realise or understand their responsibility towards Information Security. However, even if these employees knew and understood Information Security rules and regulations, they would not necessarily abide by them (IT Governance Institute, 2001a). Issues such as these led to a realisation that proper management of Information Security had to make provision also for its implementation and monitoring on a regular basis. This realisation paved the way for the “institutional wave”.

### **3.2.3 The institutional wave**

The shift from the “managerial wave” to the “institutional wave” brought about newer and better ways of securing information. Stakeholders began addressing problems that had characterised the managerial wave, such as inadequate Information Security policies. The institutional wave did not replace the managerial wave, but improved on it. Two examples of such improvements were best practices and an information security culture.

Best practices provide Information Security managers with nationally and internationally accepted guidelines for the proper implementation of Information Security in their organisations (Kwok & Longley, 1997; Von Solms & Von Solms, 2004a). It is however

important that organisations develop their own guidelines (based on existing best practices) to help them secure their information (Von Solms, 2005a).

The second improvement that was introduced in the institutional wave is the creation of an Information Security culture. This culture specifically includes the concept of the human-related issues in Information Security. Most Information Security specialists are in agreement that both the technical and the human-related (non-technical) side of Information Security should be properly tended to, because human actions cause far more damage (loss) to information than any other security threat. Even if the best technological solution to Information Security is implemented, the information is still at risk if humans are involved (Deloitte, Touche & Tohmatsu, 2005; Wood, 1995). Only if employees receive the correct and ongoing training in Information Security will the overall Information Security situation improve.

When the third wave of development of Information Security emerged, it did not replace the second wave, just as the second wave did not replace the first (Von Solms, 2000). These waves have an effect on one another, and there are issues that can be found in more than one of the development waves. For example, an Information Security policy is found in the management wave as well as in the institutional wave. The difference is that in the management wave the primary focus was on the *development* of an Information Security policy. This focus shifted in the institutional wave to create an environment where the *implementation* and *management* of the Information Security policy were given more attention. Thus it seems that a new wave improves the functionality of an existing wave.

Information Security specialists aim to keep up with the on-going development of Information Security by creating Information Security documentation that provides organisations with a vast amount of the latest knowledge regarding the management and implementation of Information Security in organisations (Smith *et al.*, 2004).

### **3.3 Information Security documentation**

Many organisations do not understand exactly how much effort is needed to secure information properly (Cutler, 2000). Organisations should treat Information Security as an ongoing process that requires a set of well-managed Information Security practices.

Authorised statements on good Information Security practices are documents prepared by Information Security specialists (Kwok & Longley, 1997). Organisations can use these Information Security documents as a starting point to determine which Information Security measures are needed to secure their information, and then they can implement and maintain such measures (Hone & Eloff, 2002; Le Grand & Ozier, 2000; Von Solms, 2000; Von Solms, 2005a). Organisations should, however, realise that they should not rely upon these documents entirely, but rather cross-reference their own guidelines to already existing standards (Kwok & Longley, 1997). Information Security documents must not be seen as a rule or procedure, but rather as a process (Kisin, 1996).

A vast amount of Information Security documentation is available today, but this thesis will provide a summary of only ten of these documents that have an exceptional reputation and are widely known in the international Information Security environment. The specification of the content of a Common Body of Knowledge for Information Security specifically for industry will accordingly be based on this Information Security documentation.

### **3.3.1 The Board Briefing Document on IT Governance**

The Board Briefing Document on IT Governance was first published in 2001 by the IT Governance Institute, which was established by the Information Systems Audit and Control Association in 1998. This document is internationally used by the Information Security community to ensure Information Security in organisations (Andersen, 2001; Kritzinger & Strous, 2002). The primary purpose of this document is to provide a guideline to the management team and technical professionals of an organisation on how to secure information in their organisation. The publication is based on the Control Objectives for Information and Related Technology (COBIT), third edition.

In this publication, enterprise governance is defined as the action that board and executive management take to provide tactical direction and ensure that the organisation's resources (as well as risk) are properly managed. This document therefore gives a great deal of attention to IT governance, which is the responsibility of the board of directors and executive management. In this publication, information is addressed as a valuable asset that must be properly protected through proper governance. Some of the

Information Security issues covered by the Board Briefing Document on IT Governance are the following (IT Governance Institute, 2001b):

- The definition of governance;
- The importance of IT governance;
- People that should be concerned with IT governance;
- Action people should take regarding IT governance.

The document concludes by explaining how an organisation may use a model to compare its current performance to that of competitors to indicate whether or not IT Governance has been implemented successfully.

### **3.3.2 The Commonwealth Protective Security Manual**

The Commonwealth Protective Security Manual was published in Australia by the Department of the Attorney General in 2000. This document is internationally known and often used by Information Security professionals to design and create Information Security policies (Allinson, 2001; McKay, 2003). Its primary aim is to provide government departments in Australia with guidance regarding the management of Information Security risks. This document includes a proper procedure designed to ensure that departments approach protective security measures in a way that is consistent throughout. The document is divided into eight parts that are numbered from A to H (Attorney General's Department, 2000).

Part A focuses primarily on a review of the Commonwealth protective security policy. It addresses important Information Security issues such as legislative requirements, roles and responsibilities regarding security in the Commonwealth, as well as maintenance and audit.

Part B provides guidelines for managing security risks. This section discusses issues such as principles of risk management and roles and responsibilities regarding security risk management in the Commonwealth. It concludes by providing a framework for risk management as well as key steps in the security risk management process.



An overview of Information Security is given in Part C. Important Information Security issues that are addressed include the roles and responsibility regarding Information Security, characteristics of integrity and availability, and procedures for protecting classified information.

Personnel security is addressed in Part D. This section addresses issues such as roles and responsibilities in respect of personnel security, determining the need for a security clearance and maintaining a security clearance.

Part E includes all Information Security issues related to physical security. Guidelines on the protection of employees and emergency management are some of the issues dealt with in this part.

Part F focuses primarily on a security framework for Competitive Tendering and Contracting (CTC). Issues addressed in this part include principles of effective CTC practices and CTC security planning.

The penultimate section of this document, Part G, is devoted to explaining the guidelines on security incidents and investigations. It includes issues such as security investigations, contact and approach reporting, and recording and reporting.

The Commonwealth Protective Security Manual concludes with Part H, which concerns security guidelines on home-based work. This includes the roles and responsibility regarding security issues of home-based work and principles for managing the security issues of such work.

### **3.3.3 The Financial Aspects of Corporate Governance Report (Cadbury Report)**

The Financial Aspects of Corporate Governance Report was first published by the Cadbury Committee in the United Kingdom in 2001. This report is accepted worldwide as an international Information Security document (Clarke, 1998; Heracleous & Luh Luh, 2002; Laing & Weir, 1999; Pass, 2004; Vinten, 2000). In the rest of this thesis this report will be referred to as the Cadbury Report. The Cadbury Report was published primarily to respond to a number of corporate failures that occurred during that period. The

document was compiled by a wide range of consultants, company directors, shareholders and professional institutes.

The main aim behind the Cadbury Report is to improve effective and proper governance within large organisations (Committee of the Financial Aspects of Corporate Governance, 1992). The report clearly specifies that top management is directly responsible for protecting the organisation's information. Top management should therefore ensure that all relevant controls and procedures are in place and working properly. Top management's actions are subjected to laws and regulations. The document provides clarity to top management, shareholders and auditors on how to establish trust within the organisation. Organisations with an established trust environment are more likely to gain the confidence of investors in the businesses community. The report also includes issues such as proper awareness and training among all stakeholders.

### **3.3.4 The Governance, Control and Audit for Information and Related Technology (COBIT) document**

The Governance, Control and Audit for Information and Related Technology (COBIT) document is a well-known and internationally accepted Information Security document that is most often implemented in large organisations (Gincel, 2004; Hone & Eloff, 2002; Le Grand & Ozier, 2000; Margulius, 2004). COBIT was first published in 1996 by the Information Systems Audit and Control Foundation. The third edition was published five years later by the IT Governance Institute (COBIT, 2001). The primary goal of COBIT is to provide policies and good practices to ensure security within an organisation.

COBIT consists of 34 high-level processes, but only one of these processes addresses security. This process, 'DS5', was included to ensure the security of systems. DS5 specifies that organisations should protect information against any security threat that could compromise its integrity. This process highlights virus prevention and detection as one of the key factors to achieve this goal. Logical access control and cryptographic keys are both identified as crucial factors in securing information. The document also stipulates that if an organisation uses the Internet (or any other public network), special attention should be given to implementing and maintaining firewalls.

DS5 concludes by stating that stakeholders, applications, technology, facilities and information are very important to consider when securing Information.

### **3.3.5 The Information Security Governance: Guidance for Boards of Directors and Executive Management document**

The Information Security Governance: Guidance for Boards of Directors and Executive Management document was published by the IT Governance Institute in 2001. This document is widely accepted among members of the Information Security community (Kritzinger & Strous, 2002). This publication deals with questions like ‘What is information security?’ and ‘Who should be concerned with governing Information Security resources?’ It states that the Board of Directors and Executive Management can be held accountable if the integrity, confidentiality and availability of information is compromised. This document is often used internationally in conjunction with the Board Briefing document on IT Governance (paragraph 3.3.1) due to the fact that they have the same aim and background.

One of the primary tasks of any Board or Executive Management highlighted in this document is to ensure that Information Security fits into the IT governance framework. The reason for this is that effective Information Security should be seen as both a business and a technological issue. The document concerned discusses the following aspects of Information Security and Governance (IT Governance Institute, 2001a):

- The background of Information Security governance
- A definition of Information Security governance
- The importance of Information Security governance
- The people who should be concerned with Information Security governance
- The role of the Board and Management
- The deliverables of Information Security governance
- How to successfully implement Information Security governance

The relationship between Information Security, IT governance and enterprise (or corporate) governance is clearly demonstrated and explained throughout this document. This document is concluded by identifying the important nature of Information Security monitoring and awareness in any organisation.

### **3.3.6 The Information Technology - Guidelines for Management of IT Security (GMITS) document**

The Information Technology - Guidelines for Management of IT Security (GMITS) document is a technical report produced by SC27, the subcommittee on Security Techniques of the ISO/IEC Joint Technical Committee on Information Technology. This technical report is highly regarded in the Information Security environment (Hone & Eloff, 2002; Martins & Eloff, 2001; Von Solms, 1998).

GMITS focuses primarily on the management of IT Security. The document consists of five parts that each addresses different areas of the management of IT security. These five parts are (GMITS, 2001):

- Part 1: Concepts and models for IT Security (first published 1996)
- Part 2: Managing and planning IT Security (first published 1997)
- Part 3: Techniques for the management of IT Security (first published 1998)
- Part 4: Selection of safeguards (first published 2000)
- Part 5: Safeguards for external connections (first published 2001).

In Part 1, concepts and models are addressed that are considered to be a basis for understanding IT security. This includes general management issues concerning the planning, implementation and operation of IT security. This part was written for managers responsible for IT Security.

Management and planning aspects are described in Part 2. This part is relevant to managers who are responsible for designing, implementing and testing IT systems within the organisation.

In Part 3 security techniques are described that are appropriate for use by those involved with management activities during a project life cycle, such as planning, designing and testing.

Guidance on the selection of safeguards for IT security is provided in Part 4. This guidance is provided for situations in which a decision is taken to select safeguards. This part also shows how an organising baseline manual can be produced.

The last part (Part 5) is aimed at providing guidance for the identification and analysis of the communications-related factors that are essential for establishing network security requirements, and also gives an indication of the potential safeguard areas.

### **3.3.7 The International Organization for Standardization: ISO 17799 and ISO 17799:2005**

ISO 17799 is well known internationally and currently implemented in a wide range of organisations around the globe (IAA *et al.*, 2000; Le Grand & Ozier, 2000; Martins & Eloff, 2001; Von Solms, 2000; Williams, 2001). This standard has been developed by industry and has gained international acceptance from the information security community. ISO 17799 has also been accepted by the public sector (Wills, 1999).

The ISO 17799 standard is based primarily on the British Standard BS 7799, which was published in Britain in 1995. About 130 security controls structured under ten headings are defined in this document to help organisations to identify Information Security issues that are relevant to their organisations. These headings are (British Standards Institute - BSI, 2002):

- Security policy
- Security organisation
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

The aim of BS 7799 is to allow companies that comply with this standard to show that they can ensure that confidentiality, integrity and availability are not compromised in any way (Gamma, 1999).

ISO 17799 was recently replaced with a later version of the standard (ISO 17799:2005) and ISO 27001 was subsequently published. These two documents are very similar, with the exception of one extra section in the latest version, namely “Information Security Incident Management”. The rest of the sections were renamed. The latest version of the standard also introduces a range of new controls (17 in total) to address a number of emerging issues not previously covered (ISO 17799 Newsletter, 2006).

### **3.3.8 The IT Infrastructure Library (ITIL) on Security Management document**

The Central Computer and Excommunications Agency (CCTA) published the IT Infrastructure Library (ITIL) on Security Management in 1999. CCTA’s IT Infrastructure Library on Security Management was drawn from the public and private sectors internally and is a widely implemented document (Chandler, 1998). It contains descriptions of best practices in Security Management that are meant to be of practical assistance and support to IT management. This includes explanations on how to organise and maintain the management of security of the IT infrastructure. In this document, which consists of five sections, security management is positioned within the total set of IT processes (CCTA, 1999).

The first section is a broad introduction to Information Security and includes aspects such as purpose, context, scope and target audience for Information Security.

In the second section the fundamentals of Information Security management are discussed, including aspects such as the value of information, security measures and IT security management processes. Information Security is first described from a business perspective and then from the perspective of the management of the IT Infrastructures.

The primary focus in the third section is on Information Security management. This section includes issues such as external and internal security, different layers in Information Security management and incident control.

Different security measures essential to all organisations are investigated in the fourth section, which begins with the implementation of Information Security. Other issues that

are included in this section include access controls, personnel security and audit. The importance of maintenance and reports in Information Security are highlighted in the conclusion of this section.

The last section of this document examines the guidelines for implementing proper security management. The first issue addressed in this part is awareness and the importance thereof. Other aspects that receive attention include the role of the security manager, documentation and a list of pitfalls and success factors.

### **3.3.9 The King Report**

The King Report is a South African-based report that is accepted all over the world (Posthumus & Von Solms, 2004; Vinten, 1998). The King Report (2002) was issued by the Institute of Directors and is a comprehensive document in which a Code of Corporate Governance and Conduct for companies in South Africa is recommended. The 2002 release of the King Report is a review of the 1994 version and includes new aspects that have an influence on the private as well as the public sector. The additions to the King Report were made because of international circumstances and ongoing developments in South Africa. The King Report consists of six sections that cover relevant aspects to promote the highest possible standard of corporate governance (King Report, 2001).

The first section is about the responsibility of the Board of Directors for the proper governance of an organisation. Section 2 includes auditing and accounting aspects of organisations, as well as issues such as legal banking, IT and accessibility of financial information. The proper procedure for internal audits in an organisation is described in Section 3. This section includes matters such as the status of internal auditors and the role and function of internal audit. The importance of risk is explained in Section 4. Aspects included in this section are the responsibility for risk management and application of risk management. Section 5 deals with the different non-financial matters in the organisation such as ethics, safety and health, intellectual capital and societal and transformation issues. The King Report concludes with a section on compliance and enforcement, and addresses matters such as the role of the media and the way forward.

Although there is no single section in the King Report that covers Information Security separately, different Information Security aspects such as ethics and the responsibility of the Board of Directors for Information Security, are integrated in the different sections.

### **3.3.10 The National Institute of Standards and Technology (NIST) Handbook**

The National Institute of Standards and Technology (NIST) Handbook has been accepted by a wide range of Information Security specialists as a guide to securing information (Dwan, 2001; Fumy, 2004). In the final draft of March 1995, the USA National Institute of Standards and Technology (2000) states that the main aim is to give support in securing all resources by introducing different Information Security concepts. The Handbook recognises that Information Security is a vital part of proper management within the organisation. It provides a solid introduction to Information Security as well as professional guidelines for properly securing information as a resource.

The NIST Handbook consists of four sections (National Institute of Standards and Technology, 2000). The first section provides a background and overview of basic Information Security issues such as Information Security definitions. This is followed by a brief discussion of Information Security risks and threats. The last part of the first section identifies the roles and responsibilities of each stakeholder within the organisation as well as to the extent to which the organisation should be involved.

The second section in the NIST document concerns management controls. Important Information Security issues such as policies, risk management and the computer system life cycle are also discussed. The section concludes with assurance aspects of the Information Security environment.

The third section focuses mainly on the operational controls in an organisation. Important issues that are described in detail include user issues, incident handling and preparing for contingencies and disasters. The most important part of this section concerns the awareness, training and education of users regarding Information Security issues in the organisation.



The document is concluded by Part 4, which is about the Technical Controls. Aspects handled in this last part are identification and authentication, logical access control, audit trails and cryptography.

### **3.4 Common Body of Knowledge for Information Security**

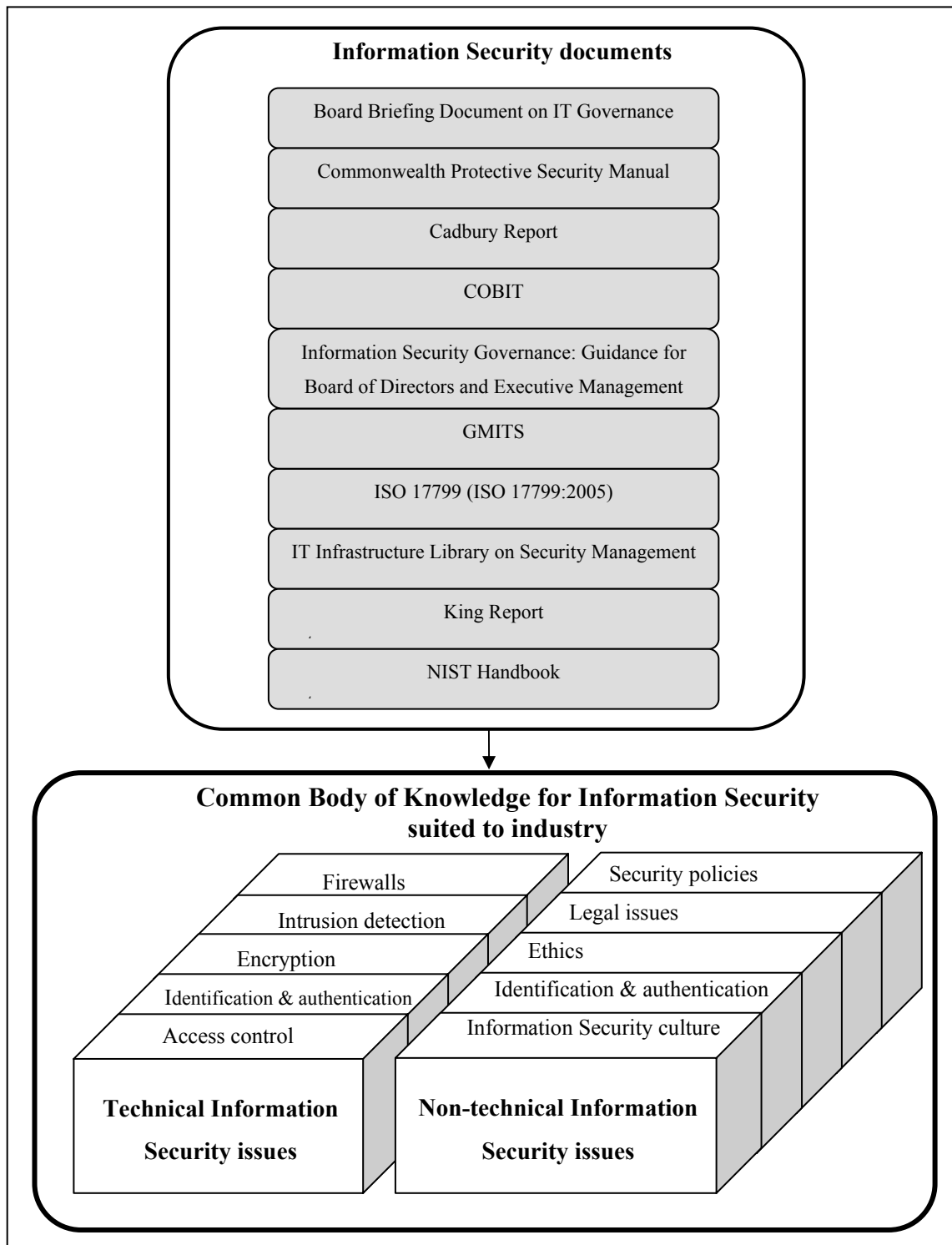
A vast amount of knowledge about Information Security can be gathered from these Information Security documents with a view to establishing a Common Body of Knowledge for Information Security. A Common Body of Knowledge is formed when national and international information is grouped together to be used as guidelines on how to secure information (Fraser, Kohane & Long, 1997). Note, however, that a universally accepted Common Body of Knowledge for Information Security does not exist yet, but there are ongoing efforts to establish one (Crowley, 2003; Wilson & Hash, 2005). A lot of work has been done in government, industrial and academic sectors and each sector has developed one or more Common Bodies of Knowledge from their own unique perspective (Crowley, 2003). These Common Bodies of Knowledge will differ from organisation to organisation, depending on their operational Information Security needs.

#### **3.4.1 A Common Body of Knowledge for Information Security suited to industry**

The Information Security Retrieval and Awareness (ISRA) model proposed in this thesis focuses specifically on developing a Common Body of Knowledge for Information Security that is *tailored for industry*. A limitation that occurs in current developments of a Common Body of Knowledge for Information Security suited to industry is that such a Body of Knowledge frequently focuses on *professionals* in industry and leaves no room or opportunity *for low-level users* (such as end users) who require a scaled-down version of this knowledge (CSI/FBI, 2005; Wilson & Hash, 2005). The aim of the Common Body of Knowledge developed as part of the Information Security Retrieval and Awareness model proposed in this thesis is, on the one hand, to focus specifically on users with little or no formal background on how to properly secure information they work with, but on the other hand, not to exclude professionals.

Another limitation in current Common Body of Knowledge for Information Security developments towards industry is that very often the non-technical, human-related issues such as ethics and legal issues do not receive as much attention as the technical issues. Specialised attention is given to technical issues where little is said about non-technical, human-related issues that play a huge role in securing information (Deloitte, Touche & Tohmatsu, 2005; Posthumus & Von Solms, 2004; Siponen, 2000a; Wright, 1998). The technical and non-technical issues of Information Security should be balanced to ensure that technical issues do not overshadow the non-technical issues and that the human side of Information Security is adequately addressed when developing a Common Body of Knowledge for Information Security suited to industry. Such a Body of Knowledge should be based on leading national and international Information Security documents to ensure that all Information Security issues (technical as well as non-technical) are dealt with.

In this chapter a Common Body of Knowledge for Information Security tailored towards industry is constructed with a view to addressing both of the limitations in current developments of such Common Bodies of Knowledge mentioned above – see Figure 3.2.



*Figure 3.2: Common Body of Knowledge for Information Security suited to industry*

The proposed Common Body of Knowledge for Information Security suited to industry is depicted in Figure 3.2. The ten nationally and internationally accepted Information Security documents summarised in paragraph 3.3 were used to establish such a Common Body of Knowledge for Information Security. There is a clear distinction between

technical Information Security issues and non-technical, human-related Information Security issues. By dividing the proposed Common Body of Knowledge into technical Information Security issues and non-technical Information Security issues, both limitations of current developments in a Common Body of Knowledge for Information Security suited for industry are addressed. Firstly, this division will ensure that those Information Security issues relevant to *low-level users* can be identified more easily, because such issues will fall primarily under the non-technical side of the proposed Common Body of Knowledge. Secondly, such a division ensures that the technical Information Security issues do not overshadow the non-technical ones.

Note that the Information Security issues depicted in Figure 3.2 do not represent an exhaustive list of technical and non-technical Information Security issues, but are merely examples of some of the issues.

The technical Information Security issues (such as those depicted in Figure 3.2) focus mainly on the technical-oriented knowledge and tools (such as encryption techniques) that are required to secure and protect information (Smith *et al.*, 2004). These issues are usually confined to the technical departments and employees with proper Information Security knowledge and work experience. Such knowledge is normally obtained through formal qualifications such as tertiary degrees/diplomas or industry-related Information Security courses.

The non-technical Information Security issues include all the non-technical-oriented knowledge that is required to secure and protect information and information systems. It includes issues such as ethics, legal issues and Information Security culture. This non-technical part can also be viewed as falling under the management side of securing and protecting information and information systems. Its focal area is the different effects that humans can have on the security and protection of information and information systems. These human influences can be classified as intentional or accidental and may come from outside as well as inside an organisation.

It is important to note that some Information Security issues may possibly fall in both the technical and the non-technical categories of the Common Body of Knowledge for

Information Security suited to industry – for example, password protection (see Figure 3.2). Password protection can be viewed as a *technical* issue in instances where technical personnel install software on the network to regulate the use of passwords. On the other hand, password protection may also be considered a non-technical issue in a situation where it is up to the user to choose a secure password. In the majority of cases, however, Information Security issues will fall under either the technical *or* the non-technical side of the Common Body of Knowledge for Information Security suited to industry. The Information Security Retrieval and Awareness model proposed in this thesis will focus exclusively on the *non-technical* Information Security issues. The primary reason for this decision is the fact that the technical Information Security issues originated during the technical wave (see paragraph 3.2.1) and a lot of research has already been done regarding implementation of these issues in industry. The non-technical Information Security issues, however, only started to emerge during the management and institutional waves (see paragraphs 3.2.2 and 3.2.3) and, in comparison with the technical Information Security issues, the human-related Information Security issues have always been neglected (CSI/FBI, 2005; Deloitte, Touche & Tohmatsu, 2005).

The *non-technical* part of the proposed Common Body of Knowledge for Information Security suited to industry therefore forms a building block for the Information Security Retrieval and Awareness model proposed in this thesis. This non-technical part of the proposed Common Body of Knowledge for Information Security suited to industry will be investigated in detail when the scope of the model is defined in Chapter 6.

### 3.5 Conclusion

Chapter 3 gave an overview of the on-going development of Information Security. The developments regarding Information Security were grouped according to three so-called waves, namely the technical, management and institutional waves. These three waves are not isolated, but influence and complement one another. Information Security will keep evolving as new threats arise with the development of better and new technologies.

This chapter also provided a summary of ten state-of-the-art nationally and internationally accepted Information Security documents, created by Information Security specialists in an attempt to keep up with these developments. The purpose of

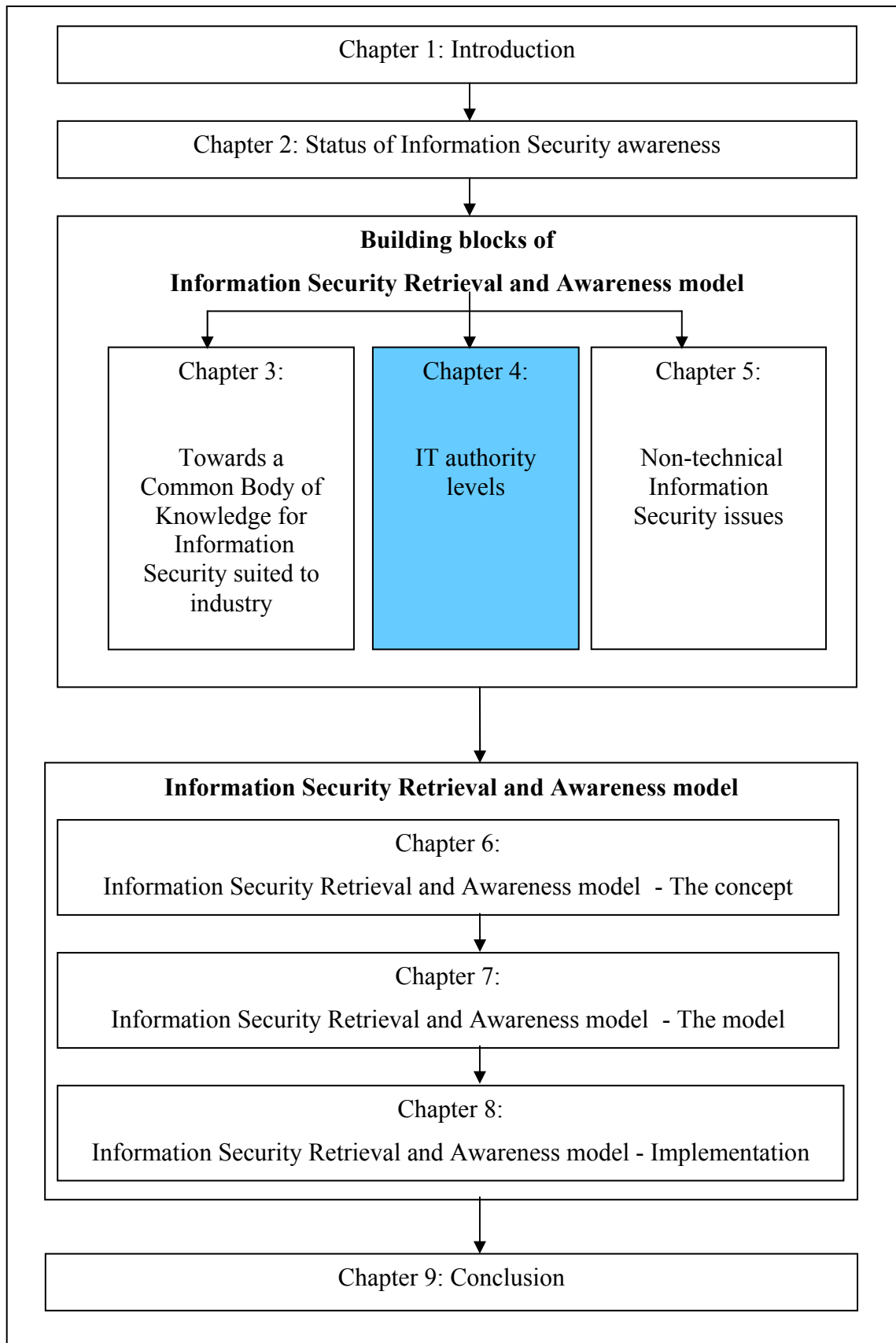
these documents is to provide guidelines to organisations on how to properly secure their information. These Information Security documents form the basis for a Common Body of Knowledge for Information Security suited to industry proposed in this chapter.

The proposed Common Body of Knowledge was subsequently divided into technical Information Security issues and non-technical Information Security issues. All stakeholders in an organisation – i.e. those with little or no technical background, as well as professionals – should be aware of one or more of the Information Security issues that form part of the proposed Common Body of Knowledge for Information Security tailored towards industry.

In the next chapter (Chapter 4), the different groups of stakeholders in industry are identified and grouped together according to their job category. Each of these groups will have a different responsibility towards securing the information within the organisation and accordingly should be aware of those Information Security issues related to their job category only.

# **Chapter 4**

## **IT authority levels**





## 4.1 Introduction

It is essential to incorporate nationally and internationally accepted Information Security documentation in an organisation's Information Security plan so as to ensure that acceptable Information Security controls and standards are implemented in the organisation (Andersen, 2001; Kisin, 1996; Posthumus & Von Solms, 2004; Von Solms, 2001a). Information Security documentation is, however, usually extensive and contains a huge amount of information that is not relevant to *all* stakeholders in the organisation. Different groups of stakeholders should be identified and relevant Information Security roles and responsibilities should accordingly be assigned to each group. This will ensure that a specific group of stakeholders is not burdened with an enormous amount of Information Security documents that might include a large amount of irrelevant information, but receives only the essential information needed to secure the specific information the group works with. The author refers to such groups as IT authority levels.

The purpose of this chapter is to identify the different stakeholders in a typical organisation and to group these stakeholders according to the different IT authority levels that are most common in industry. In this way suitable nationally and internationally accepted Information Security documents relevant to each IT authority level can be identified.

## 4.2 Grouping of stakeholders

All organisations comprise of stakeholders. These stakeholders are the people who ensure the survival of the organisation (National Institute of Standards and Technology, 2000). To provide a clear explanation of the different stakeholders in a typical organisation, let us consider the following example:

John and Peter (two stakeholders) decide to start a small business – FURNITURE FOR AFRICA – that sells and delivers office furniture. Both decide that they will be involved in all the overall decision-making processes, but not in the overall management of the business. They therefore appoint Maggie (another stakeholder) to be in charge of the day-to-day management of the business. Maggie will be responsible for ensuring that all decisions made by John and Peter are properly implemented and enforced by all stakeholders.

FURNITURE FOR AFRICA will be based in Johannesburg, South Africa, and the furniture warehouse will be in Pretoria, South Africa. A decision is made to appoint two managers; Muzi will manage the shop and Jo the warehouse and both will report to Maggie.

A proper network infrastructure is needed between the shop and the warehouse. Two stakeholders, William and Sam, are appointed to set up the network connection between the shop and the warehouse, as well as maintain it. William and Sam have sufficient working experience and knowledge to be appointed as technical employees.

Anne is appointed as the security manager and must ensure that the information in the organisation is secured at all times. She should therefore ensure that neither the availability, confidentiality nor integrity of information is compromised in any way. Anne is responsible for developing and implementing a proper Information Security policy and for monitoring the implementation of the policy.

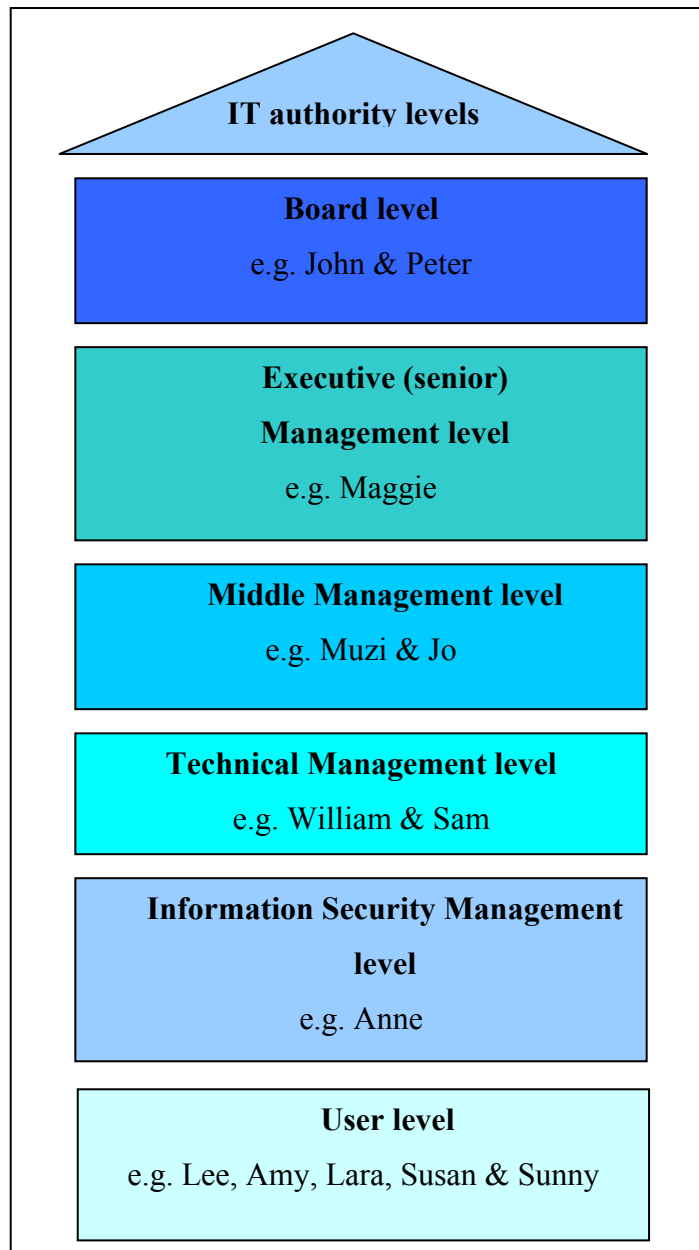
The last stakeholders appointed (Lee, Amy, Lara, Susan and Sunny) are employees who will be responsible for day-to-day activities such as secretarial work and sales. These stakeholders usually have little or no knowledge of Information Security issues.

All the stakeholders (as mentioned above) who work for FURNITURE FOR AFRICA can be grouped into different IT authority levels. There are many different ways to group stakeholders to form different IT authority levels in industry (National Institute of Standards and Technology, 2000). Stakeholders in an organisation can be grouped according to the specific stakeholder's job function or job category, or according to the technology and products used by the stakeholder (National Institute of Standards and Technology, 2000). The *job function* refers to a specific function that a stakeholder performs, such as developing the security policy of the organisation. If stakeholders are grouped according to job function, the organisation will have a larger number of IT authority levels, but each level will have a small number of stakeholders with specialised skills. This is different to grouping stakeholders according to *job category*, for example executives, where the organisation will have a small number of IT authority levels, but with a larger number of stakeholders on each level. Finally, stakeholders can also be grouped according to the *technology and products* they use (such as word-processing

packages), but this grouping may need to be changed often as a new product or technology becomes available.

The author will use the second method, i.e. *job category*, to group the different stakeholders. An IT authority level will therefore comprise of one or more stakeholders in the same job category. This method has been used widely in industry as well as by Information Security professionals and is best suited to the proposed Information Security Retrieval and Awareness model for industry (International Federation of Accountants, 2000; Kisin, 1996; National Institute of Standards and Technology, 2000; Siponen, 2001; Thomson, 1999; Whiteman & Mattord, 2003).

When creating IT authority levels according to job category, one should remember that job category in organisations will differ from organisation to organisation and therefore the IT authority levels will also be different from one organisation to the next (Kisin, 1996; National Institute of Standards and Technology, 2000; Siponen, 2001; Thomson, 1999; Whiteman & Mattord, 2003). For the purpose of this thesis, the IT authority levels of a typical organisation are identified as depicted in Figure 4.1. Note that the IT authority levels illustrated in Figure 4.1 are not the only IT authority levels that can be found in a typical organisation, but for the purpose of the proposed Information Security Retrieval and Awareness model these are sufficient. More IT authority levels can be added later to the proposed model if needed. For the sake of clarity, the names of the stakeholders of the FURNITURE FOR AFRICA example are also included in Figure 4.1 under the relevant IT authority level.



*Figure 4.1: IT authority levels*

Each of the IT authority levels depicted in Figure 4.1 above can also be subdivided into more detailed IT authority levels. Consider for example the user level. This level can be divided into two levels. The first sublevel consists of the *users of information*, i.e. stakeholders who use information provided by the computer. The second sublevel is comprised of *users of systems*, i.e. as stakeholders who use the computer system directly (National Institute of Standards and Technology, 2000). It is up to each individual organisation to decide if it requires subdivisions at a specific IT authority level or not. For the purpose of this thesis, the main levels as depicted in Figure 4.1 are sufficient.

## 4.3 Information Security responsibilities of IT authority levels

This paragraph will focus primarily on the Information Security responsibilities assigned to each IT authority level. The responsibilities assigned to the IT authority levels may differ between organisations and should be structured to suit the organisation's needs. Each of the IT authority levels depicted in Figure 4.1 will be addressed individually in the remainder of this chapter.

### 4.3.1 Board level

The three top IT authority levels (Board level or Board of Directors, Executive Management level and Middle Management level) depicted in Figure 4.1 have Information Security responsibilities that will overlap. However, the Board level is ultimately responsible for ensuring that information in the organisation is not compromised in any way. It is the responsibility of the Board to ensure that proper Information Security policies are designed and implemented in the organisation.

The Board level is widely recognised as the highest IT authority level of a typical organisation (Kisin, 1996; National Institute of Standards and Technology, 2000; Siponen, 2001; Thomson, 1999; Whiteman & Mattord, 2003). In the FURNITURE FOR AFRICA example, John and Peter are responsible for the decision-making processes. Their decisions, such as implementing an Information Security awareness programme, should improve the security of information. Being the highest authority in an organisation, the Board is ultimately responsible for the management and safekeeping of *all* information recourses (Lewis, 2000). The Board should therefore ensure that Information Security governance is enforced throughout the organisation (Andersen, 2001; IT Governance Institute, 2001a; Lindup, 1996; Von Solms, 2001a). Information Security governance is enforced by law in many countries and in such cases the Board can be taken to court and held accountable if the integrity, availability or confidentiality of information is compromised in any way (Lindup, 1996). The Board level should therefore protect information through effective management that is assured only through effective Board supervision (Von Solms, 2001a). They should be informed about all Information Security issues in the organisation in order to address Information Security in all aspects of the organisation (IT Governance Institute, 2001a).

The Board level should play a proactive role in Information Security to ensure that the rest of the IT authority levels will follow (National Institute of Standards and Technology, 2000; Whiteman & Mattord, 2003).

### **4.3.2 Executive (senior) Management level**

The second IT authority level (depicted in Figure 4.1) is the Executive Management level. This level will typically include the Chief Executive Officer (CEO), who is directly accountable to the Board level. The Executive Management level will work very closely with the Board level and many of their responsibilities will overlap, such as ensuring proper Information Security governance within the organisation (Andersen, 2001; IT Governance Institute, 2001a). The Executive Management level should therefore ensure that the decisions taken at Board level are executed properly.

Executive Management should set a good example for all stakeholders by adhering to all the appropriate security practices in the organisation. Security policies and procedures mean nothing if the top IT authority levels do not practise what they preach (Forcht, 1994; National Institute of Standards and Technology, 2000). Executive Management (with the help of the Board and Middle Management levels) should therefore ensure that Information Security is taken seriously in the organisation by all stakeholders, by ensuring that proper Information Security policies and procedures are implemented and regularly monitored by relevant stakeholders (Kisin, 1996; Nosworthy, 2000; Siponen, 2001).

In the FURNITURE FOR AFRICA example, Maggie is the Executive Manager and she is responsible for providing supervision of a comprehensive Information Security programme.

### **4.3.3 Middle Management level**

Middle Management (the third IT authority level depicted in Figure 4.1) usually consists of different Heads of Departments or sections, and differs from one organisation to the next. This level should ensure that all Information Security policies and procedures are being implemented correctly and enforced by those stakeholders who fall under their responsibility (Nosworthy, 2000). The Middle Management level should also ensure that the Information Security roles and responsibilities of such stakeholders are defined and

correctly assigned (IT Governance Institute, 2001a). It is therefore the responsibility of Middle Management to ensure that all Information Security policies that are provided by the Board and Executive Management levels are implemented and maintained at lower levels. The Middle Management level reports directly to the Executive Management level.

In the FURNITURE FOR AFRICA example, Muzi and Jo operate at Middle Management level and they should ensure that there is an open line of reporting, directly to the Executive Management level, regarding all Information Security issues and incidents (Kritzinger & Von Solms, 2004).

### **4.3.4 Technical Management level**

The fourth IT authority level (depicted in Figure 4.1) is the Technical Management level, which consists of stakeholders who are managers or technicians who design and operate computer systems in the organisation (National Institute of Standards and Technology, 2000). This level is one of the most important levels to properly secure information and has been around since the inception of Information Security (International Federation of Accountants, 2000; Kisin, 1996; Siponen, 2001; Thomson, 1999).

The Technical Management level ensures that all technical aspects, such as the latest information technologies and associated vulnerabilities and risks, are addressed promptly and correctly by implementing and maintaining proper Information Security measures. This will ensure that the integrity, availability and the confidentiality of information is maintained at all times. The stakeholders on this IT authority level should have thorough Information Security knowledge and considerable work experience. This knowledge is usually obtained through formal qualifications such as tertiary degrees/diplomas or industry-related Information Security courses. The Technical Management level reports directly to the Middle Management level.

In the example of FURNITURE FOR AFRICA, William and Sam are responsible for establishing technical communication between the shop and the warehouse. This connection will include computer hardware and software, as well as an in-depth knowledge of technical Information Security issues such as firewalls, encryption and network configurations.

### 4.3.5 Information Security Management level

The Information Security Management level (the fifth IT authority level depicted in Figure 4.1) is widely recognised as the level that directs the day-to-day management of Information Security in the organisation (International Federation of Accountants, 2000; Kisin, 1996; National Institute of Standards and Technology, 2000; Siponen, 2001). This level is primarily responsible for the assessment, management and monitoring of *security measures* in the organisation (Whiteman & Mattord, 2003). The Information Security Management level should report directly to the Middle Management level regarding issues such as implementing, updating and monitoring of Information Security policies in the organisation. The Information Security Management level, in collaboration with Middle Management, should ensure that all stakeholders are aware of their role and responsibility towards securing information they work with. This can be achieved through a well-designed Information Security retrieval and awareness programme that is implemented and monitored on a regular basis.

In the example of FURNITURE FOR AFRICA, Anne is responsible for ensuring that all possible security measures are set in place to secure information. Anne is also responsible for ensuring that all Information Security policies and procedures are implemented correctly. For example, Anne should ensure that the organisation's day-to-day Information Security measures, such as the Information Security awareness programme, are functioning as they should. The Information Security Management level reports directly to the Middle Management level.

### 4.3.6 User level

The last IT authority level depicted in Figure 4.1 is the User level. All stakeholders who fall under a specific User level have a responsibility for securing the information they use (National Institute of Standards and Technology, 2000; Wood, 2004). These stakeholders should be made aware of all Information Security rules and regulations regarding the proper securing of the information they work with (International Federation of Accountants, 2000; Kisin, 1996; Siponen, 2001; Thomson, 1999; Yngstrom & Bjorck, 2004). Information Security awareness programmes are vital at this level, because many users have little or no formal background on how the information they work with should



be secured. The User level reports mostly to the Information Security Management level regarding Information Security issues.

In the example of FURNITURE FOR AFRICA, the stakeholders at the User level are Lee, Amy, Lara, Susan and Sunny who should be aware of all relevant Information Security policies and procedures related to the information they work with, and implement them on a day-to-day basis.

### **4.4 Summary of Information Security responsibilities**

Having discussed the responsibilities of each IT authority level, it becomes evident that there are functions and responsibilities among the top three management levels (Board, Executive Management and Middle Management) that overlap. This is due to the fact that these levels work very closely together to provide a global exposure to Information Security in the organisation.

Figure 4.2 provides a summary of the primary responsibilities regarding Information Security of each IT authority level (as depicted in Figure 4.1).

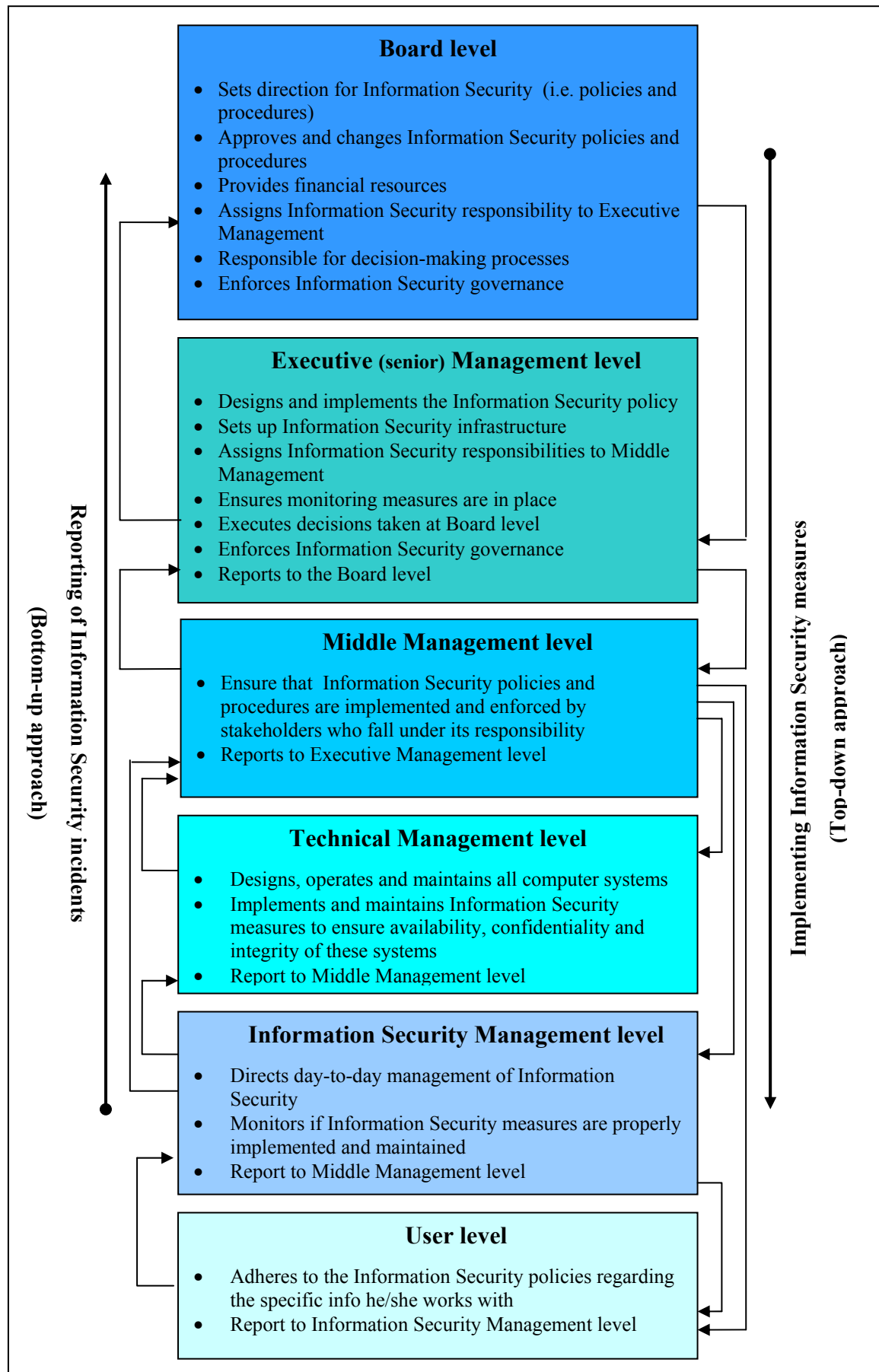


Figure 4.2: Information Security responsibilities of IT authority levels

A top-down approach should be followed towards implementing Information Security. According to such an approach, the roles and responsibilities regarding Information Security are prearranged and enforced by an IT authority level with greater authority than the level below. For example, the Board level is responsible for approving the Information Security policy, whereas Executive and Middle Management are responsible for implementing such policy in the organisation. It is therefore clear that all IT authority levels should be proactively involved in Information Security in the organisation.

The reporting of Information Security incidents, however, should follow a bottom-up approach. In this way, all IT authority levels provide information regarding Information Security incidents directly to their appointed manager, i.e. an IT authority level at a level higher. For example, if a user detects a virus on his/her computer, he/she must immediately inform the Information Security management level, who will handle the incident accordingly. The Information Security management level, in turn, will report all security incidents to a higher authority level, namely to Middle Management. This approach will ensure that all Information Security situations and incidents are reported to the Board level, which has the authority to change the Information Security policies or procedures if necessary.

### 4.5 Conclusion

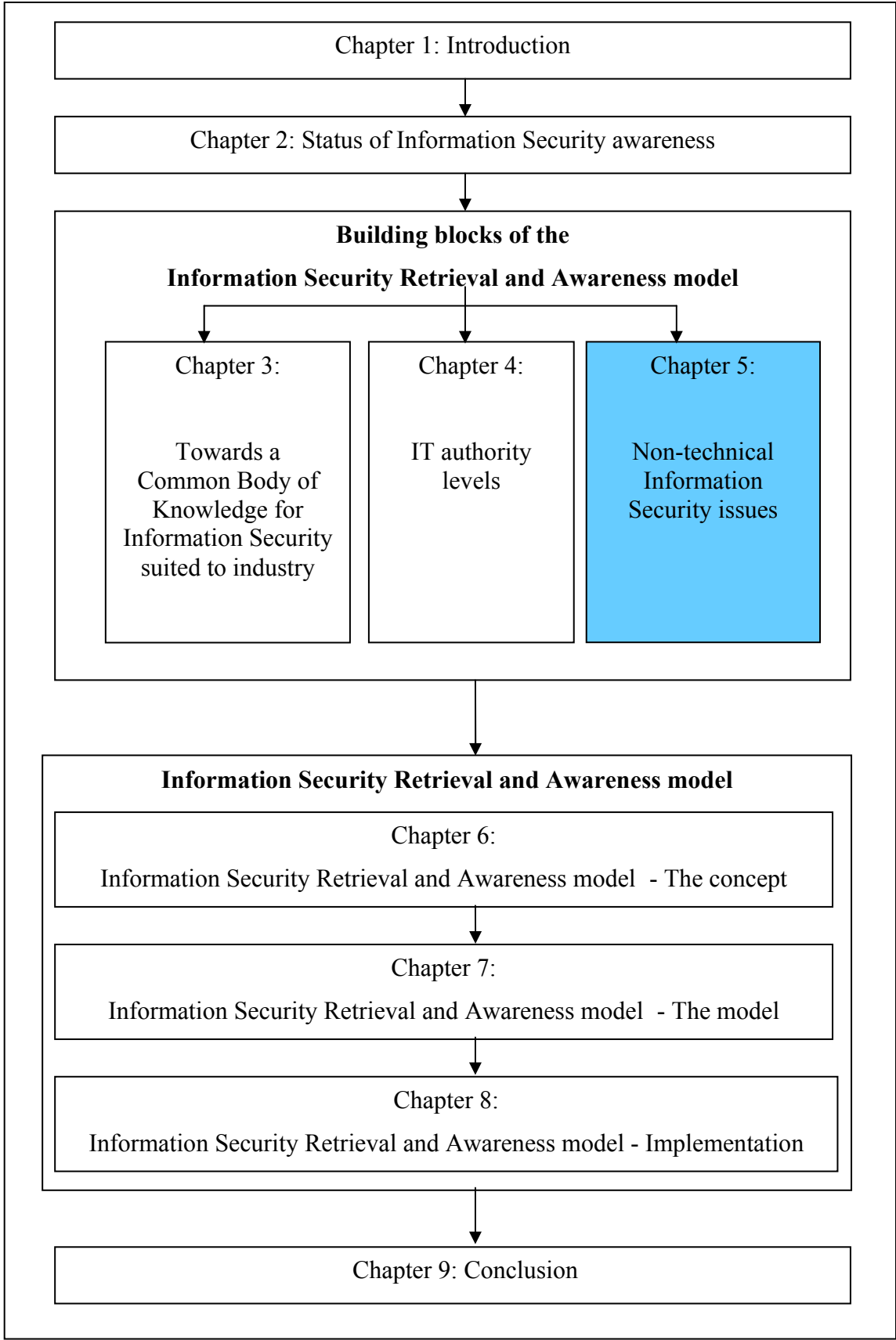
In this chapter, different groups of stakeholders that can be found in a typical organisation were identified and grouped according to their job category. These groups (which each comprises one or more stakeholders) are referred to as IT authority levels. Each of these IT authority levels has its own role and responsibility towards securing information. Stakeholders within each level should therefore be made aware of the different Information Security issues relevant to securing the information they work with. Identifying different stakeholders and grouping them into IT authority levels will ensure that stakeholders on each level are not burdened with unnecessary information. The IT authority levels identified in this chapter will form an integral part of the proposed Information Security Retrieval and Awareness model.

The next chapter, **Chapter 5**, investigates the different non-technical, human-related Information Security issues that IT authority levels should be made aware of. These non-

technical Information Security issues form part of the non-technical part of the Common Body of Knowledge for Information Security suited to industry (proposed in Chapter 3), which will constitute one of the building blocks of the proposed Information Security Retrieval and Awareness model.

# **Chapter 5**

## **Non-technical Information Security issues**



## **5.1 Introduction**

Each IT authority level should be made aware of the specific Information Security issues that are directly related to its specific job category – as discussed in Chapter 4. This can be achieved by extracting all the information regarding the relevant Information Security issues from the Common Body of Knowledge for Information Security suited to industry (as presented in Chapter 3), for each separate IT authority level. In this way stakeholders are not weighed down with irrelevant information.

Chapter 5 will discuss all the different *non-technical* Information Security issues that form part of the Common Body of Knowledge for Information Security (as depicted in Chapter 3). These non-technical Information Security issues refer to the *type* of non-technical, human-related knowledge relating to Information Security that is required to secure the IT environment. The list of non-technical Information Security issues discussed includes most issues that are addressed in the nationally and internationally accepted Information Security documents discussed in Chapter 3 (paragraph 3.3). Note, however, that Information Security is an evolving field, and this list of issues should therefore be updated on a regular basis to ensure that all new non-technical Information Security issues are promptly addressed and managed. The non-technical Information Security issues discussed in the remainder of this chapter will be used as another building block in designing and creating the proposed Information Security Retrieval and Awareness model for industry.

## **5.2 The non-technical Information Security issues**

Many of the non-technical Information Security issues such as ‘risk management’ have been around for a number of years and been a regular topic of research. Mostly all of the non-technical Information Security issues originated in either the management or the institution wave (see Chapter 3, paragraphs 3.2.2 and 3.2.3). Some of the other issues such as ethics only started to become important as a result of the development of new technologies over the last few years.

### 5.2.1 Risk management

*Risk management is the process of ensuring that risks within the organisation are kept and maintained at an acceptable level* (National Institute of Standards and Technology, 2000).

Risk is about the likelihood of damage, loss or injury and can be found in any organisation. An example of such a risk is if an employee compromises his/her password. The impact of this is that an unauthorised person can access secured information and compromise the integrity, availability or confidentiality of the information. These risks should therefore be identified and managed in order to keep security losses to a minimum (Burnette, 2005; Gerber & Von Solms, 2005; Whiteman & Mattord, 2003).

Risk management consists of specific phases, namely risk identification (identifying all possible risks), risk assessment (estimating the probability that risk could occur), risk analysis (making decisions regarding Information Security based on the outcome of the risk assessment) and risk monitoring (monitoring the risk situation in the organisation to identify any changes) (Smith, 2000). The aim of risk management is to minimise risk or, in the best case, to prevent risks from occurring. Each stakeholder in the organisation should in some way be involved in managing risks in the organisation (Whiteman & Mattord, 2003).

Risk management can be seen as a technical as well as a non-technical Information Security issue. The *technical* side of risk management involves issues such as installing firewalls to ensure that no unauthorised person could obtain access to the system. The *non-technical* side of Risk management involves issues such as management decision making processes.

### 5.2.2 Information Security management

*Information Security management is about maintaining the state of Information Security in an organisation* (Pfleeger, 1997; Whiteman & Mattord, 2003).

Information Security management is a growing issue in all business spheres and affects management positions at all different IT authority levels, from the User level to the Board



level. Information Security management is about ensuring the identification and authentication, authorisation, confidentiality, integrity and non-repudiation of information through proactive management and through understanding the risks, threats and vulnerabilities. All employees of an organisation should understand the importance of Information Security management and how they (as employees) are responsible for their actions in the workplace.

Information Security management should be an ongoing process within the organisation. This ongoing process must be built into day-to-day business operations instead of being treated as an optional extra (Lewis, 2000). If organisations implement Information Security management as a daily issue, they will develop an all-round Information Security management culture that will enhance all-round Information Security among stakeholders.

### **5.2.3 Corporate governance (including Information Security governance)**

*Corporate governance is the system or method by which companies are directed, controlled and managed* (Cadbury Report, 1992; Lindup, 1996; Moulton & Coles, 2003; Turnbull, 2003).

Corporate governance must be taken seriously due to the fact that the accountability for corporate governance ultimately rests with the Board level and the Executive Management level (Von Solms, 2001b). If the corporate governance system fails, international scandals can occur such as that involving ENRON. ENRON is an American company that went bankrupt in 2002 as a result of unacceptable corporate governance. Corporate governance must therefore be taken seriously in order to ensure the survival of the organisation.

Corporate governance is a responsibility enforced by law in countries such as South Africa and England. The Board level and Executive Management level are also accountable for the proper *Information Security governance* in organisations. *Information Security governance* involves the leadership, organisational structure, processes and technologies that ensure that the confidentiality, integrity and availability of the

organisation's electronic assets are maintained at all times (Von Solms, 2001b). The Board level and Executive Management level can be taken to court if the integrity, availability or confidentiality of information is compromised in any way. Consequently these management levels in many large organisations are now expressing a much greater interest in Information Security than a few years ago (Kwok & Longley, 1997). They have never been as dependent on Information Security as they are today (Lindup, 1996; Von Solms, 2005b). All the signs show that this dependency can only increase. It is essential that corporate governance include Information Security as a vital part of governing an organisation and that the Board level and Executive Management level should also encourage effective and responsible use of information among all stakeholders in the organisation.

### 5.2.4 Legal issues

*Legal issues are part of the legal system that different countries put in place to adapt to advancing technologies and human behavior (Aljifri & Navarro, 2003).*

Over the past decades new technologies have opened new doors and possibilities for opportunists to commit crimes. As a result of new technologies (like the Internet) thousands of computers are connected all around the globe. A person in South Africa can communicate with someone in Alaska as if they were in adjoining rooms. However, no matter how easy and convenient the Internet is, it is not always safe. We are bombarded daily with stories of different crimes that have been committed over the Internet. These computer crimes range from hacking, viruses, fraud and sabotage to theft committed by anybody – from amateurs to organised crime groups. There are thousands of examples of computer crimes committed over the last few years. One of them involved the Melissa viruses that cost organisations around the world more than \$1.5 trillion in 2000. It is therefore vital to recognise the importance of Information Security legislation and how it influences the way information is secured (Briney, 2003; Edwards, 2003; Verine, 2004).

Although computer crimes are legally wrong, there are a lot of cases that still fall within grey areas of the law. For example, if a person in South Africa hacks into a computer in America, in which country can he/she be held accountable? The country he/she resides in or the country in which he/she committed the crime? Something that receives much attention is the issue of privacy. Privacy prevails when a person can be certain that his/her

personal information is kept private. Someone's privacy can be affected if, for example, his/her credit card is stolen on the web and used for something else. Such a case occurred in March 2000 when two people were arrested in Sicily after having stolen about 1 000 credit card numbers on the Internet and using them to purchase lottery tickets. Some countries (such as the United Kingdom, USA, Canada, Denmark, France, Norway, Sweden and Germany) are consequently starting to see the privacy of people in a new light. Data privacy legislation in these countries states that companies must inform employees that their computer and Internet use is being monitored. This is not only a problem at national level – it must also be addressed at organisational level. Organisations should take responsibility for securing the information they have.

A survey carried out in Britain revealed that the people responsible in nine out of ten attacks on the Internet were not prosecuted (Reim, 2000). Examples such as these illustrate that there are still many legal decisions that need to be made in the computer security environment. The evolution of legislation on international level is very slow. A report prepared by McConnel International (2000) analysed the state of the law in 52 countries. The report found that only ten of these nations had amended their laws to cover more than half of the kinds of crimes that had to be addressed. Some of the countries that had by then updated their laws to some extent included Denmark, Spain, the United Kingdom and China. According to the report countries such as France, New Zealand, Norway and South Africa had no updated laws. Thus many countries were and still are behind in respect of the updating and enforcing of computer law.

### 5.2.5 Computer ethics

*Ethics can be seen as a set of prescribed rules or a code of behavior that is used to distinguish between right and wrong (Raikow, 2000; Rossouw, 2002; Seifried, 2000). Computer ethics is when the ethical rules or code of behavior are implemented within the computer environment (Rossouw, 2002).*

Computer ethics is probably one of the most recent additions to the management of Information Security. Computer ethics relates to the interaction between man and computers. A great deal has already been published on ethics in general, but *computer ethics*, in particular, has not had similarly wide exposure. The rapid growth of technology in today's computer environment brings new ethical dilemmas. One example of such an

ethical dilemma is whether or not it is ethical to use other stakeholders' access codes to obtain classified data. Different stakeholders can be expected to give different answers to this question. Since their answers will depend on personal factors, such as religion and background, people may have different standards about what is acceptable or unacceptable in society (Seifried, 2000). Many of these ethical dilemmas still fall within a grey area and most of the time computer professionals may not be prepared to deal effectively with the ethical issues that arise in their workplace (Maner, 1996).

Computer ethics must not be seen as a legal issue – though something may be legal, it does not necessarily mean it is ethical (Rossouw, 2002; Seifried, 2000). So what distinguishes ethics from legal issues? Ethics concerns human morals; what is wrong and what is right according to *each one's personal ethical framework* (Rossouw, 2002). This ethical framework may differ from one person to the next, depending on a variety of different aspects such as gender, race, language, religion or culture.

The direct result of this diversity of ethical frameworks is that a situation may develop that is ethically acceptable to one person but unacceptable to another, such as surfing the Internet for personal use during office hours. These ethical issues are usually addressed in one way or another by the code of ethics that is adhered to by an organisation.

Almost all professional organisations have a code of ethics, which usually maintains that one must do what is right and report what is wrong. It is mainly the responsibility of the organisation to ensure that it has a code of ethics which is distributed to all employees. One problem with many (if not all) of these codes is that they only include the basic issue of ethics, for example rejecting bribery, while they do not include issues regarding computer ethics in particular. Computer ethics should be explicitly included in the general code of ethics of an organisation (Floridi, 2005).

### 5.2.6 Professionalism

*Professionalism is about the professional responsibility stakeholders have towards their working environment* (Little et al., 1999).

Organisations often rely on their employees to uphold the image of the organisation to ensure good relationships within the organisation as well as with clients, partners and

investors. Organisations must therefore try to develop professionalism among all their employees. Professionalism includes aspects such as competence, accountability, personal character and conduct, and loyalty. Information Technology, and specifically Information Security, requires a growing level of professionalism (Pillay, 2000).

Professionalism is a great starting point to ensure that a stakeholder will take his/her role towards securing information seriously. When they are professional, stakeholders will understand how important it is to follow set rules and maintain the highest work standard. This will heighten their sense of responsibility towards ensuring the security of the information they work with, as well as complying with all other Information Security standards set for them by the organisation.

### **5.2.7 Information Security culture**

*Information Security culture is about the way things are done regarding securing information in an organisation* (Martins & Eloff, 2002; Von Solms, 2000).

In today's ever-changing environment, organisations must try to create and sustain a healthy Information Security culture (Guant, 2000; Martins & Eloff, 2002; Nosworthy, 2000; Rash, 2004; Von Solms, 2000). An Information Security culture focuses on encouraging the proper planning and management of all information security issues in the organisation, especially since organisations are as dependent on their data, information systems and networks as they are today. Information Security must become part of the day-to-day culture (operation) of employees. Instilling a strong security culture in one's company can help to ward off hacker attacks (Fonseca, 2000). Organisations have to change their culture and keep up with current Information Security developments if they want their organisation to be secured (Rash, 2004).

Any Information Security culture is dynamic and in a constant state of flux due to the influence of new Information Security issues (such as computer ethics). This ever-changing technological environment means that what is considered to be state of the art today will be obsolete in the near future. Not only does security need to keep pace with these ongoing changes in technology, but those who work with information must also adapt on an ongoing basis (Rash, 2004). It is important that the correct behaviour towards Information Security should become part of the culture of the organisation (Martins &

Eloff, 2002). This culture must be cultivated throughout the organisation and involve all stakeholders (Le Grand & Ozier, 2000; Von Solms, 2000). Cultivating an Information Security culture among stakeholders will ensure the safety of all information resources.

### 5.2.8 Information Security policy

*An Information Security policy is defined as a document that contains specific rules and regulations regarding securing information within a specific organisation (National Institute of Standards and Technology, 2000).*

Before any organisation can start to manage their Information Security, they should first have an Information Security policy in place as a guideline to **what** must be managed and **how** this must be done. The Information Security rules and regulations stipulated in the Information Security policy relate to the hardware, software, networks and information within an organisation (Von Solms & Von Solms, 2004a; Waint, 2005). One purpose of an Information Security policy is to protect the organisation's information assets from all threats, whether internal or external. All organisations must have an information security policy in place so as to ensure that all information is correctly and fully secured. The presence of an Information Security policy is one of the most important elements in the prevention of Information Security incidents (Lewis, 2000). The assumption is then that an information security policy is no longer a luxury, but a basic necessity for any organisation wanting to secure its information.

Information Security policies lately experienced a paradigm shift. A few years ago many organisations had a properly designed Information Security policy, but were not implementing it (Doherty & Fulford, 2006; Von Solms & Von Solms, 2004b). The policy was probably stored on a shelf somewhere, instead of being used and managed. When Information Security management started to become more prominent, it was surrounded by much controversy regarding the failure to manage the Information Security policy. Critics argued that an organisation that did not manage its information security policy, might just as well not have had such a policy at all (Von Solms & Eloff, 2000).

### **5.2.9 Physical security**

Physical security controls and policies should be implemented to protect and secure the facility that houses information resources, the information resources themselves, as well as the facility used to support their operation (NIST, 2002).

It is essential that appropriate physical security and access control measures be designed and implemented within the organisation to ensure that information is safeguarded against any possible physical Information Security threats that could occur (COBIT, 2001). An example of a physical security measure is to ensure that all working areas (i.e. work stations) are property secured (i.e. locked doors) when the work area is unattended. This is to ensure that no unauthorised person gains access to the work areas (ISO/IEC177799, 2000).

## **5.3 Conclusion**

The discussion in this chapter centred around the Information Security issues that form part of the non-technical part of the proposed Common Body of Knowledge for Information Security suited to industry. These issues are human-related and usually overshadowed by the technical Information Security issues when Information Security awareness is dealt with. The Information Security Retrieval and Awareness model proposed in this thesis focuses specifically on these non-technical Information Security issues.

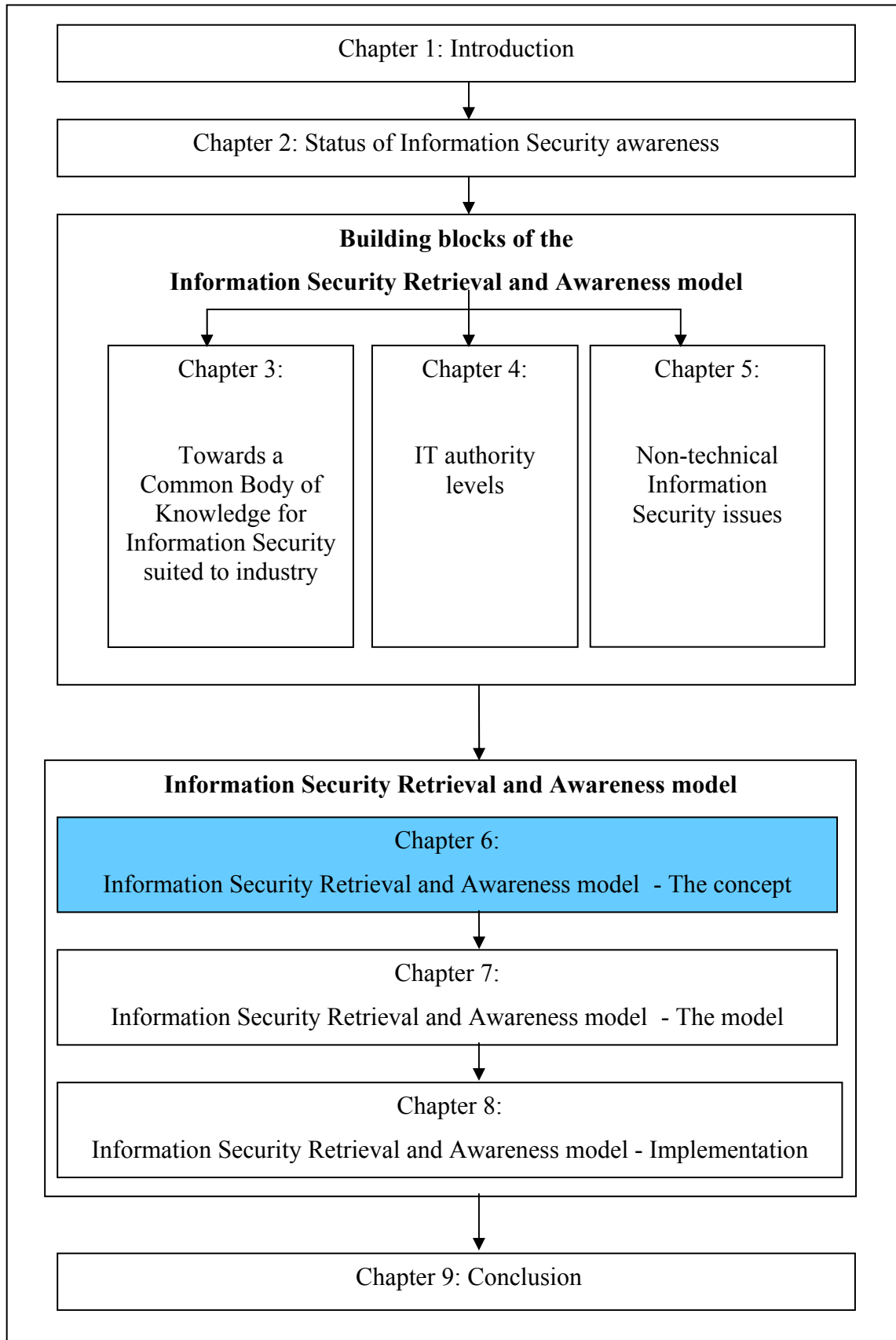
Chapter 6 is devoted to introducing the proposed Information Security Retrieval and Awareness (ISRA) model suited to industry. A conceptual view of the proposed ISRA model is presented, after which the scope of the model is investigated.

## **Chapter 6**

# **Information Security Retrieval and Awareness (ISRA) model –**

## **The concept**





## 6.1 Introduction

Information Security awareness is attracting increasingly more attention from industry, because stakeholders are held accountable for the information with which they work (Briney, 2004; CompTIA, 2006; CSI/FBI, 2005). The current status of Information Security awareness in industry indicates, however, that human-related, non-technical Information Security issues are often overlooked when a Common Body of Knowledge for Information Security is developed. Furthermore, such a Common Body of Knowledge usually focuses on the professionals in industry and pays little attention to low-level users. For this reason, the author proposes an **Information Security Retrieval and Awareness model** – entitled “ISRA” – that is tailored specifically towards industry.

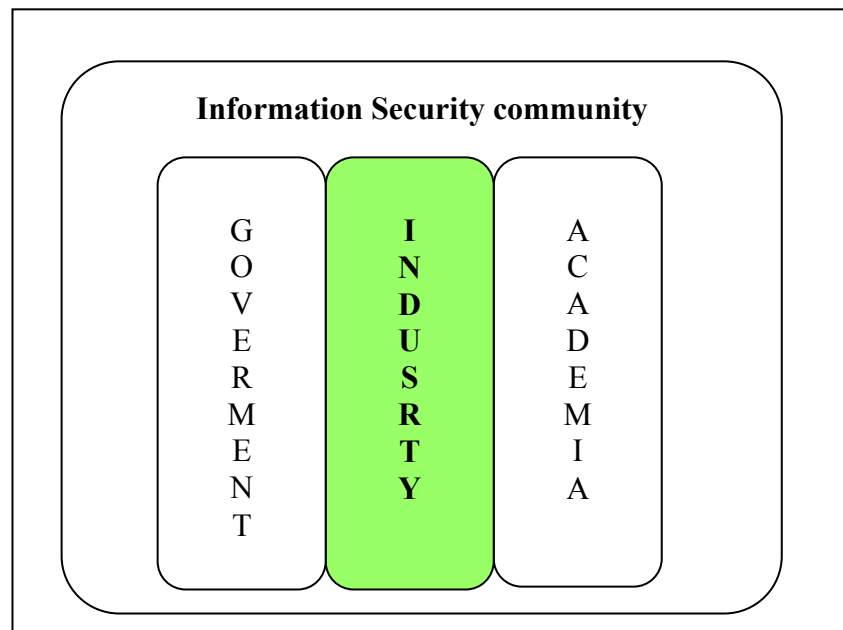
The proposed model will hopefully enhance Information Security awareness in the specific domain of industry, in the sense that it is *based on a Common Body of Knowledge for Information Security suited to industry (proposed in Chapter 3), which draws a clear distinction between technical and non-technical Information Security issues*. The ISRA model will focus exclusively on the *non-technical* Information Security issues, in order to cancel out the lack of attention to these issues as opposed to the technical Information Security issues. Furthermore, the ISRA model does not take into account only the Information Security professionals, *but incorporates all stakeholders in an organisation (including low-level users) who need to be aware of Information Security*. The model ensures that stakeholders are *made aware only of the relevant Information Security issues that they need to be aware of according to their job category*, thus preventing them from being burdened with unnecessary information. Finally, the ISRA model incorporates a retrieval component, which will *allow stakeholders to retrieve relevant information related to Information Security issues at any time*. The information retrieved through this process can, for example, assist an IT authority level (such as the Board level) in decision-making processes. For example, if the Board level is designing or reviewing an Information Security policy (such as the Information Security awareness policy), it can request a list of Information Security awareness issues that should be addressed in terms of the policy. This list is compiled by retrieving information directly from the ISRA model. It will save time and effort and the required information can be obtained immediately.

The purpose of the ISRA model proposed in this thesis is therefore not to discourage the use of existing Information Security awareness models, but rather to propose a new way of addressing and enhancing Information Security awareness in industry. The first part of this chapter is devoted to presenting the scope of the ISRA model, whereas the second part will provide a conceptual view of the multi-dimensional ISRA model.

### 6.2 Scope of the ISRA model

The scope of the ISRA model is defined in terms of, firstly, the *Information Security community* and, secondly, the *Common Body of Knowledge for Information Security*.

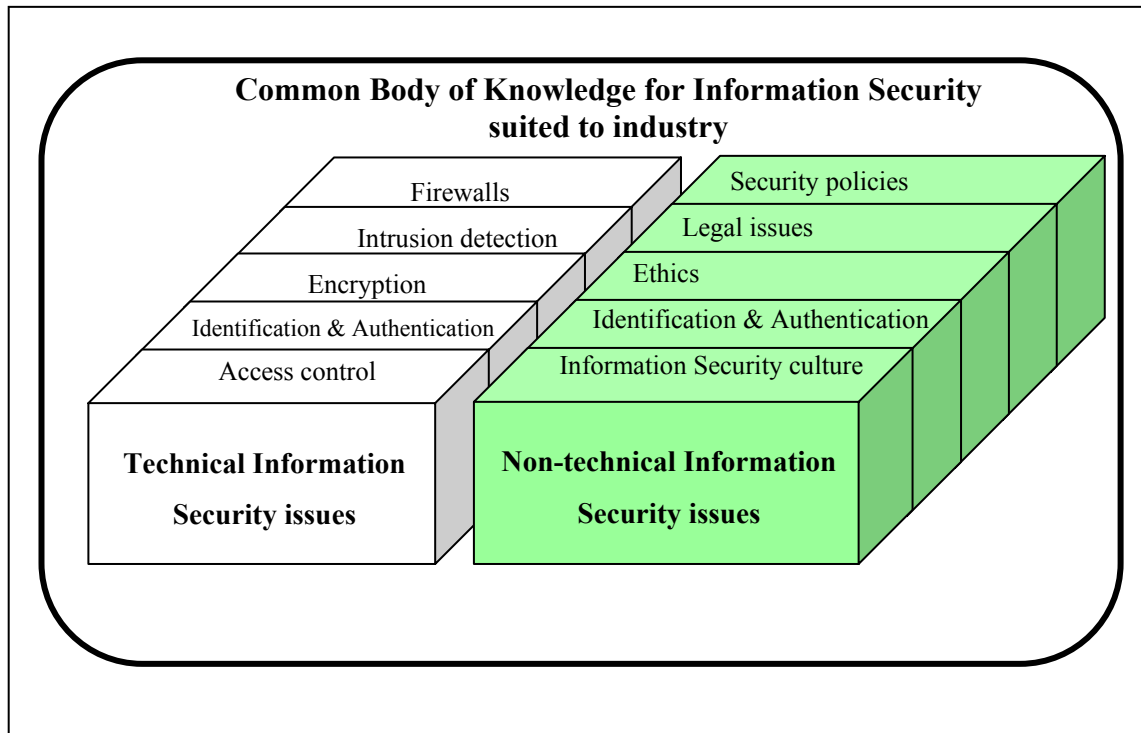
The Information Security community on which the model focuses, consists primarily of three main Information Security sectors (as discussed in Chapter 2), namely *government*, *industry* and *academia* (depicted in Figure 6.1 below) (Crowley, 2003; Hillburn, 1999). Each sector should be aware of the specific Information Security issues (technical and non-technical) relevant to their sector. The ISRA model focuses specifically on the industry sector, as indicated by the shaded area in Figure 6.1.



**Figure 6.1: The Information Security community – Scope of the ISRA model**

The scope of the ISRA model is also defined in terms of the Common Body of Knowledge for Information Security. Such a Common Body of Knowledge specifically suited to industry was proposed in Chapter 3. The ISRA model focuses primarily on *the*

*non-technical* Information Security issues that are relevant to stakeholders in industry, as indicated by the shaded area in Figure 6.2.



*Figure 6.2: The scope of the Common Body of Knowledge for Information Security suited to industry*

The aim of focusing on the non-technical Information Security issues is to counterbalance the traditional under-emphasis of non-technical Information Security research and implementations (Corporate Governance Task Force Report, 2004; CSI/FBI, 2005; Eloff & Eloff, 2005; Posthumus & Von Solms, 2004; Wood, 2004). It should be noted, however, that the technical Information Security issues are equally important, but do not form part of the scope of the ISRA model.

## **6.3 Conceptual view of the ISRA model**

### **6.3.1 Three-dimensional approach**

Designing and creating Information Security awareness models for industry is not something new and can be done in many different ways (Pratt, 2006; Schou, 2001; Thomson, 1999).

One way of designing Information Security awareness models is to follow a *one-dimensional* approach (Katsikas, 2000; Schou, 2001). For example, Schou (2001) addresses only the different *Information Security issues* needed to secure information. In an academic environment such a one-dimensional approach could well be acceptable for providing a broad overview of Information Security to learners. It is however not adequate at industry level.

Another way of designing Information Security awareness models is to follow a *two-dimensional* approach (Crowley, 2003; Hesse & Smith, 1999; National Institute of Standards and Technology, 2000; Nosworthy, 2000; Thomson, 1999). Such an approach incorporates both *Information Security issues* and *stakeholders*. This approach specifies the Information Security issues that are important and the stakeholders to whom these issues are important. The author is of the opinion that at industry level even a two-dimensional approach is inadequate. The reason is that the *content* of the Information Security issues is not addressed. One of the aims of the ISRA model is to refrain from burdening stakeholders with irrelevant information, but rather to provide them with the specific content relating to non-technical Information Security issues relevant to their specific IT authority level. Such content can be retrieved from nationally and internationally accepted Information Security documents. The ISRA model therefore follows a *three-dimensional* approach by including these documents.

The three dimensions can be summarised as follows:

The first dimension includes the different *Information Security issues* that form part of the scope of the ISRA model – as depicted in Figure 6.2.

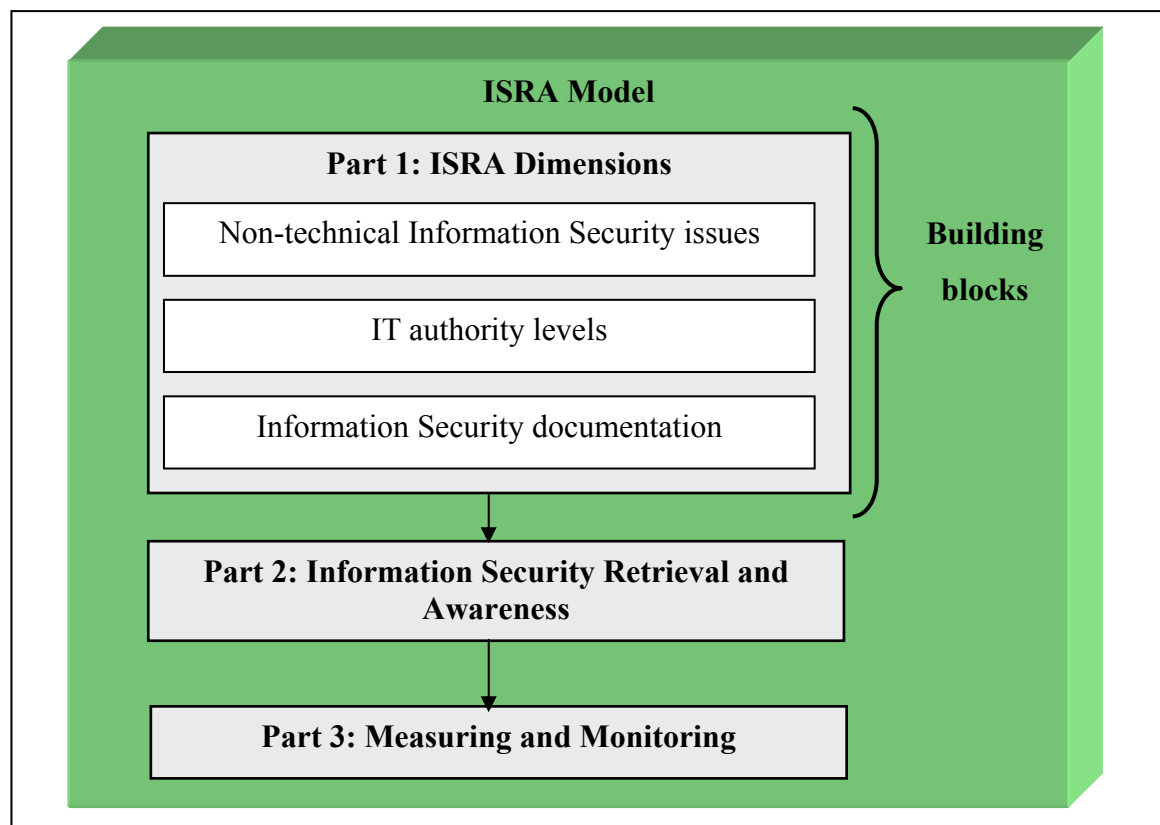
The second dimension includes the different *IT authority levels* (consisting of stakeholders as discussed in Chapter 4) to which the content of the relevant Information Security issues should be made available. This will ensure that all stakeholders in the organisation (Information Security professionals as well as low-level users) are exposed to the non-technical Information Security issues relevant to their IT authority level.

The third dimension consists of national and internationally accepted *Information Security documents* that contain state-of-the-art information regarding the implementation and management of Information Security issues. The ten leading Information Security documents discussed in Chapter 3 will be included in the ISRA model.

The three dimensions mentioned in this paragraph are subsequently integrated to form the building blocks of the ISRA model.

### 6.3.2 The ISRA model

A conceptual view of the ISRA model is depicted in Figure 6.3.



*Figure 6.3: Conceptual view of the ISRA model*

The ISRA model consists of three parts, the *ISRA Dimensions*, *Information Security Retrieval and Awareness* and *Measuring and Monitoring*.

As is illustrated in Figure 6.3, the ISRA dimensions form the building blocks of the ISRA model. This is the area in which all information regarding Information Security awareness is accumulated. The ISRA model follows a three-dimensional approach and

therefore integrates the dimensions of the *non-technical Information Security issues*, *IT authority levels* and *Information Security documents*. These dimensions will be used as the foundation for the second part of the ISRA model, namely Information Security Retrieval and Awareness.

The second part of the ISRA model will focus primarily on retrieving relevant information from the ISRA dimensions. This relevant information will be requested by IT authority levels, depending on their Information Security awareness needs. The information retrieved in this part will be used to enhance Information Security awareness among all IT authority levels, as well as to assist IT authority levels when involved in decision-making processes.

The purpose of Part 3 of the ISRA model – Measuring and Monitoring – is to help organisations to measure the current status of Information Security awareness in the organisation, and to monitor the rapid developments in the Information Security field to ensure that all new Information Security issues are incorporated and addressed.

### 6.4 Conclusion

This chapter provided an overview of the scope and concept of the ISRA model. The model is developed for industry and focuses on the non-technical Information Security issues. It consists of three main parts, namely *ISRA dimensions*, *Information Security Retrieval and Awareness* and *Measuring and Monitoring*. The first part of the three-dimensional approach comprises of non-technical Information Security issues, IT authority levels and state-of-the-art Information Security documentation.

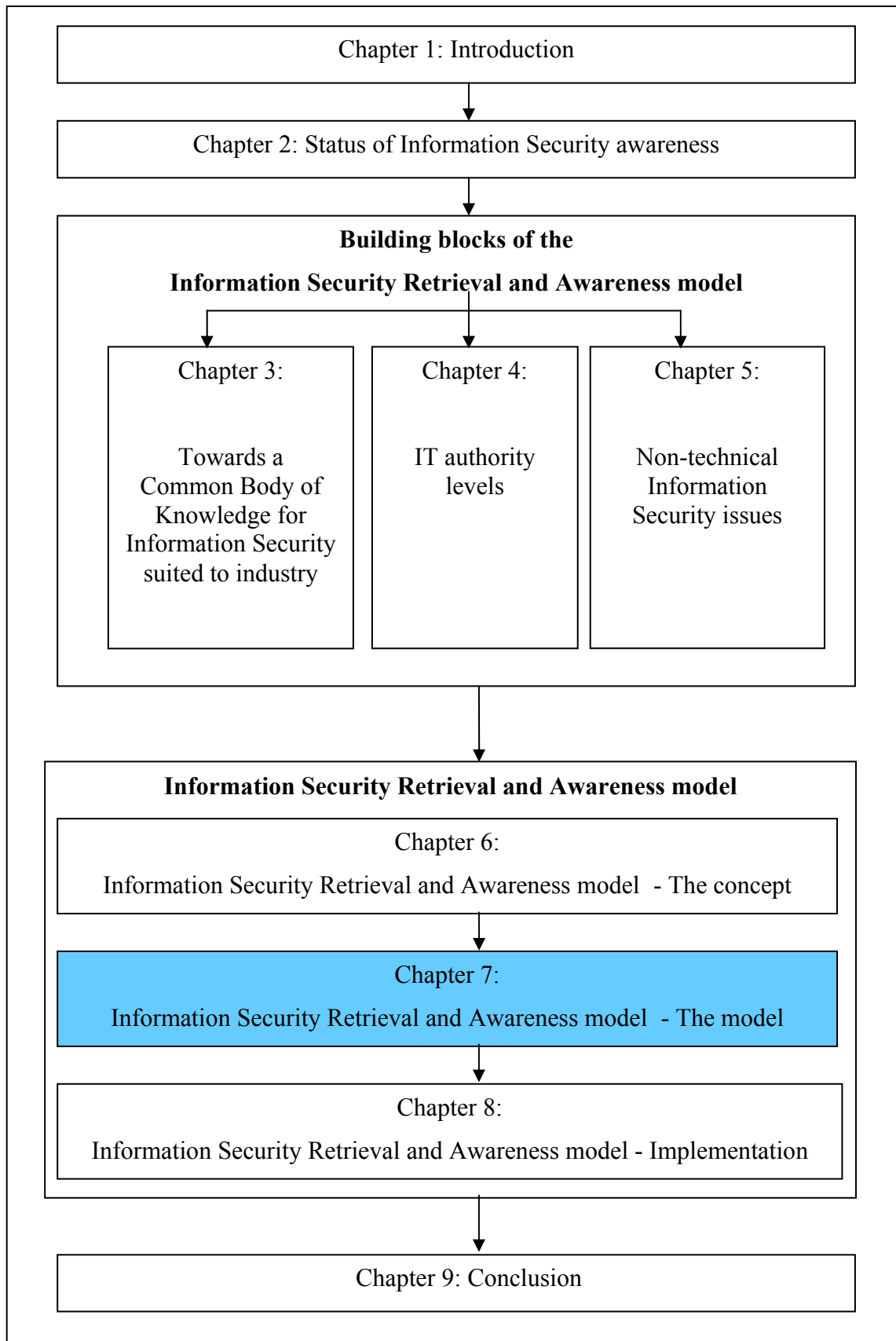
Chapter 7 will be devoted to a detailed discussion of the three main parts of the ISRA model.

## **Chapter 7**

# **Information Security Retrieval and Awareness (ISRA) model –**

## **The model**





## 7.1 Introduction

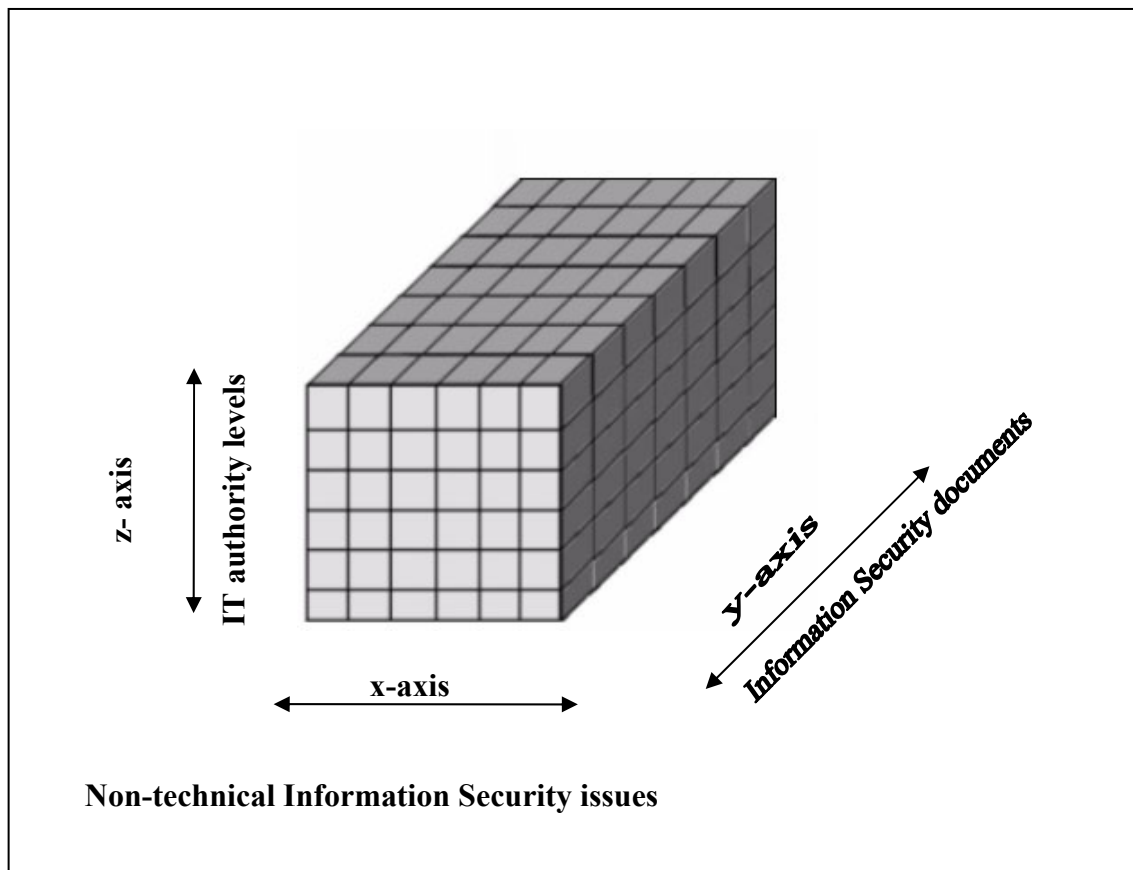
In Chapter 6, the concept of the proposed ISRA model was introduced. The scope of the model was highlighted and an overview of the three main parts of the ISRA model, i.e. ISRA Dimensions, Information Security Retrieval and Awareness, and Measuring and Monitoring, was provided. The ultimate aim of the ISRA model is to enhance Information Security awareness among employees. Statistics show that about 35% of Information Security incidents originate inside organisations (Deloitte, 2005; CIO & PriceWaterhouseCoopers, 2005). Organisations should therefore realise that they have a responsibility to raise their internal Information Security awareness in order to minimise such incidents.

This chapter will be devoted to an expansion of the ISRA model by discussing each part of it in detail.

## 7.2 Part 1: ISRA Dimensions

As discussed in Chapter 6, the ISRA model follows a three-dimensional approach towards Information Security awareness by incorporating the following three dimensions: *Information Security documents*, *IT authority levels* and *non-technical Information Security issues* - as graphically depicted in Figure 7.1. These three dimensions constitute the first part of the ISRA model.

The first dimension – *Information Security documents* – is represented on the **y-axis**. The second dimension – *IT authority levels* – is represented on the **z-axis**, while the third dimension – *non-technical Information Security issues* – is represented on the **x-axis**.



*Figure 7.1: Graphical view of the ISRA Dimensions*

The aim of the ISRA Dimensions is to organise information regarding Information Security in such a way that retrieval of this information is fast and easy for all stakeholders.

The ten nationally and internationally accepted state-of-the-art Information Security documents that form the basis of the proposed Common Body of Knowledge for Information proposed in Chapter 3 (paragraph 3.3), will be used to populate the Information Security documents dimension of the ISRA model. The different IT authority levels (stakeholders grouped according to job category) identified in Chapter 4 will be used to populate the IT authority levels dimension of the ISRA model. Finally, the different non-technical Information Security issues as discussed in Chapter 5 will be used to populate the non-technical Information Security issues dimension of the ISRA model. The ISRA Dimensions will be used as the building blocks for the next part of the ISRA model (i.e. Information Security Retrieval and Awareness).

## 7.3 Part 2: Information Security Retrieval and Awareness

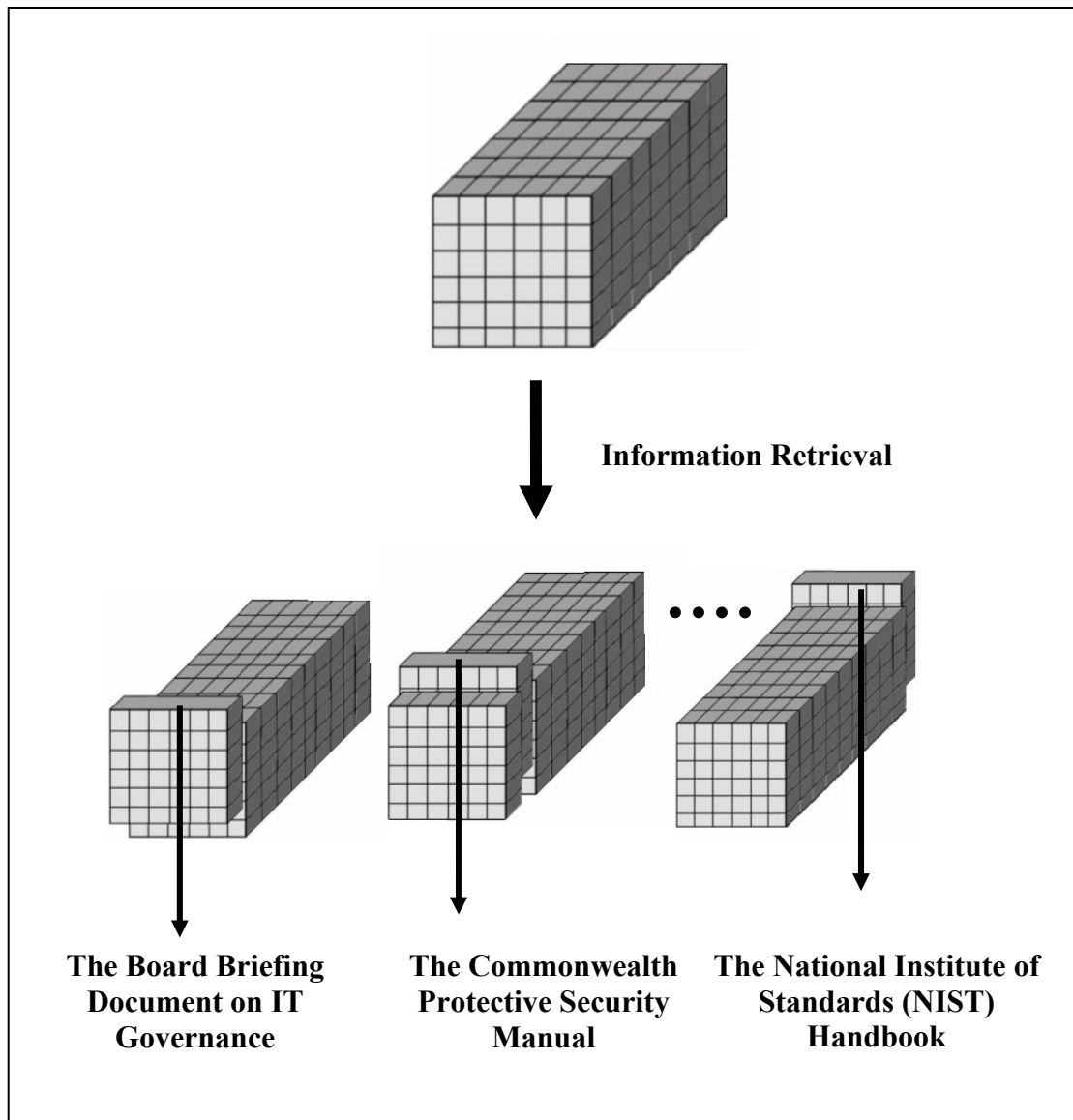
The second part of the ISRA model involves Information Security Retrieval and Awareness, and uses the ISRA Dimensions to retrieve the relevant information requested by stakeholders. The ISRA model encourages such participation by allowing the stakeholders to become familiar with relevant Information Security issues in their own time and at their own pace. This is done by providing stakeholders with various options for retrieving and studying Information Security issues without the need to involve another person.

The advantage of representing the ISRA dimensions in a three-dimensional way (as depicted in Figure 7.1) is that the information within the dimensions can be viewed from different angles or viewpoints. For example, information regarding a specific Information Security document can be obtained by viewing the ISRA dimensions from the y-axis, z-axis or a combination of x-, y- or z-axes. Accordingly, three different ‘slicing methods’ will be used to retrieve relevant information from the ISRA Dimensions.

### 7.3.1 y-Slicing

The author refers to the first slicing method as the ‘y-slicing method’. This method extracts all requested information regarding individual **Information Security documents** from the ISRA dimensions. Each y-slice will represent **one** document, which includes the relevant information from the other two dimensions (IT authority levels and non-technical Information Security issues). Therefore, the y-slicing method will indicate the non-technical Information Security issues that are important (relevant), as well as the IT authority level for which they are important (relevant), based on a specific Information Security document. This slicing method is depicted in Figure 7.2.

In the example depicted in Figure 7.2, the first slice represents the information obtained from the Board Briefing Document on IT Governance; the second slice represents information obtained from the Commonwealth Protective Security Manual, and so forth.



*Figure 7.2: y-slicing*

Figures 7.3 to 7.12 show the relevant information that is obtained for each Information Security document by means of the y-slicing method. In these figures the ○ symbol is used to indicate the IT authority level that is *ultimately responsible* for that specific non-technical Information Security issue – according to the specific document. The ◎ symbol is used to indicate the IT authority level that should ensure that the *implementation* of a specific non-technical Information Security issue is completed – according to the specific document. Finally, the ● symbol indicates that a specific IT authority level should only be *aware* of that non-technical Information Security issue – according to the specific document.

Consider for example Figure 7.3. It represents the slice that is obtained by way of the y-slicing method for the first Information Security document, namely the Board Briefing Document on IT Governance. According to this document, the Board level and Executive Management levels are ultimately responsible for ensuring that risk management and corporate governance are adequately addressed within an organisation.

Figure 7.4 represents the slice that is obtained via the y-slicing method for the second Information Security document, namely the Commonwealth Protective Security Manual. According to this document, the Board level and Executive Management levels are ultimately responsible for risk management, corporate governance, the Information Security policy and physical security. Furthermore, all of the IT authority levels should be aware of pertinent legal issues. Lastly, Middle Management, Technical Management, Information Security Management and Users should be made aware of the Information Security policy and physical security within the organisation.

The y-slicing method is applied to the remaining Information Security documents in a similar way as was explained in respect of the Board Briefing document on IT Governance and the Commonwealth Protective Security Manual. (See Figures 7.4 to Figure 7.12.)

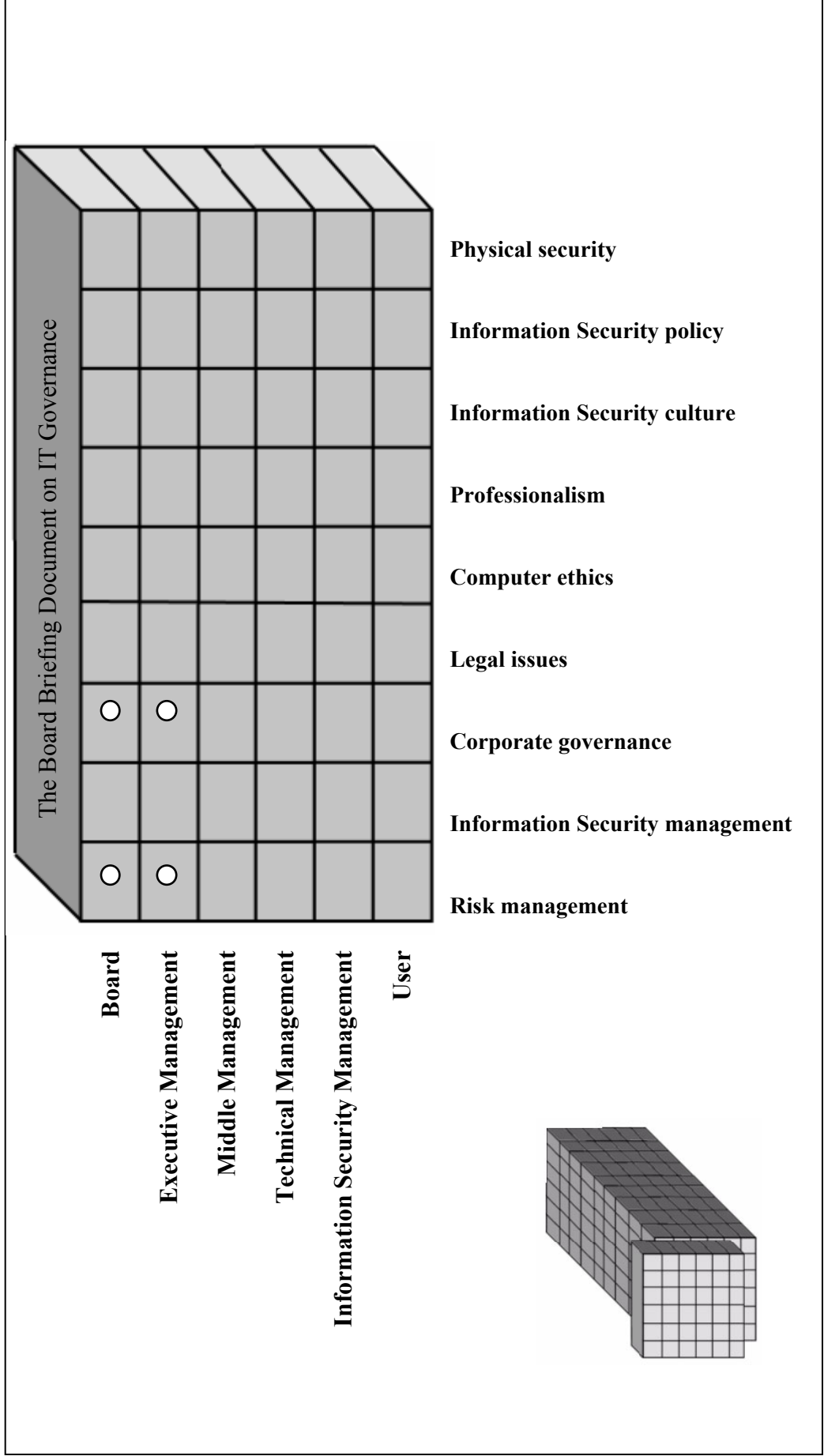


Figure 7.3: The Board Briefing Document on IT Governance

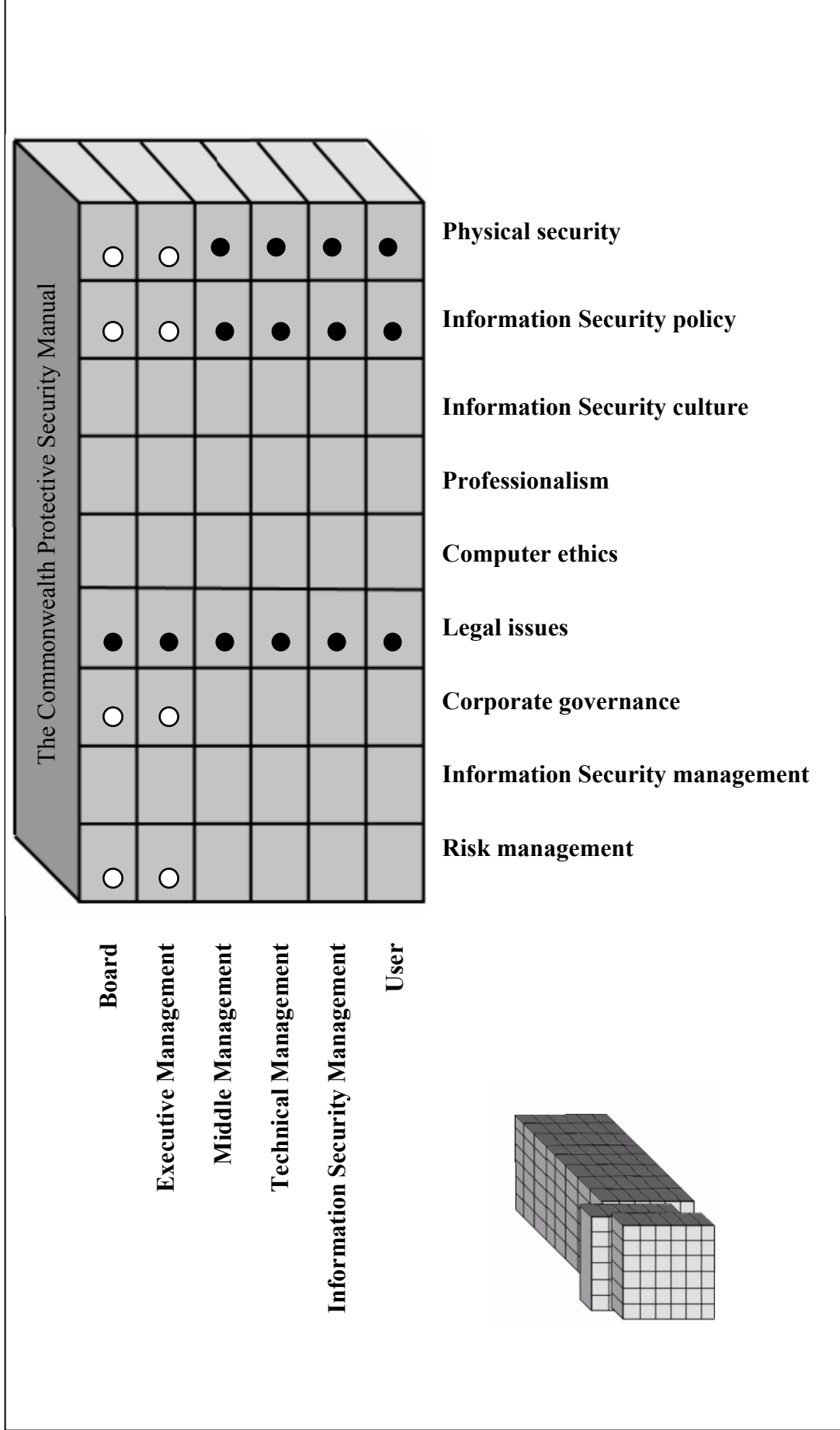


Figure 7.4: The Commonwealth Protective Security Manual



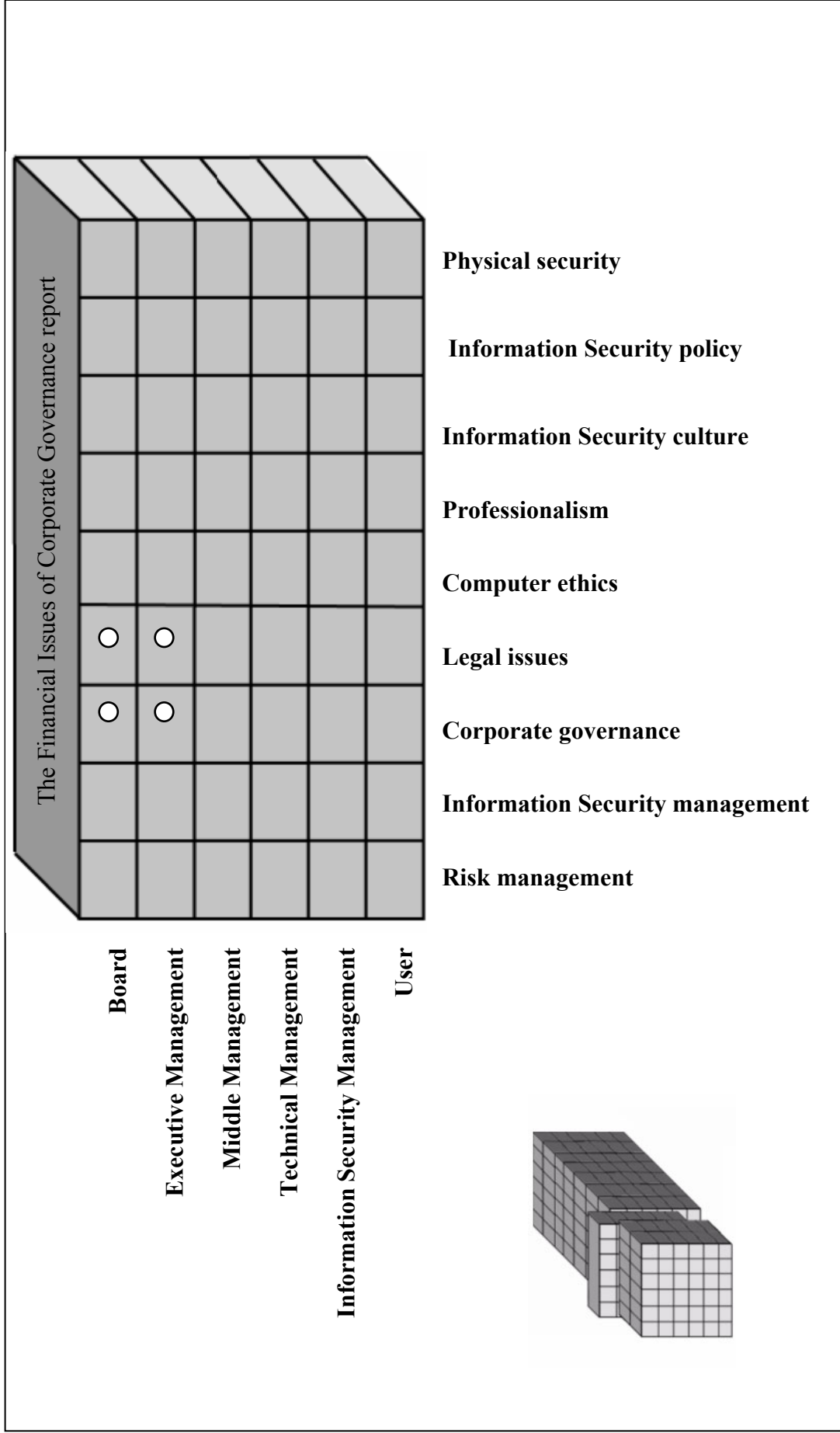


Figure 7.5: The Financial Issues of Corporate Governance report (Cadbury Report)

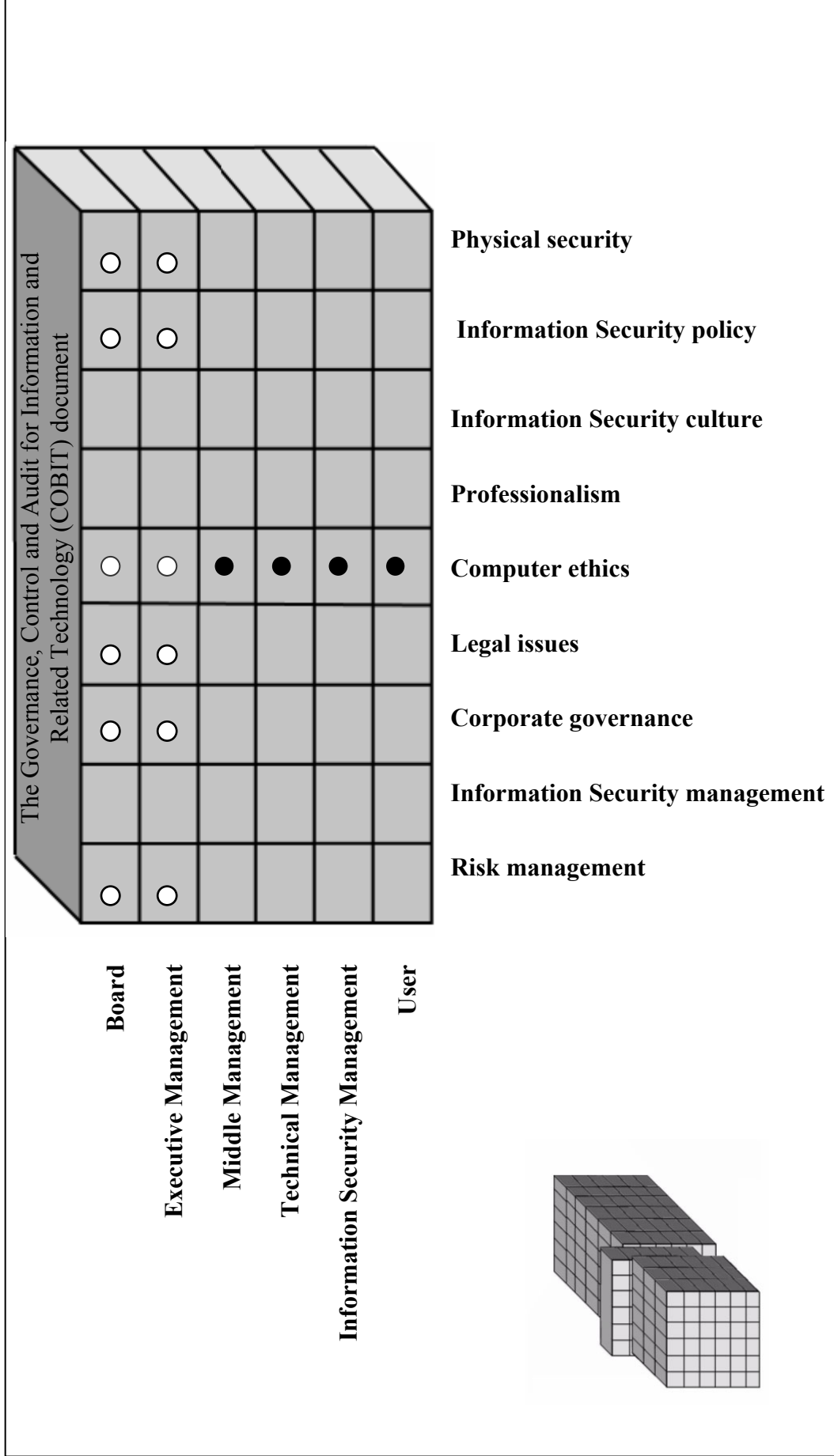


Figure 7.6: The Governance, Control and Audit for Information and Related Technology (COBIT) document



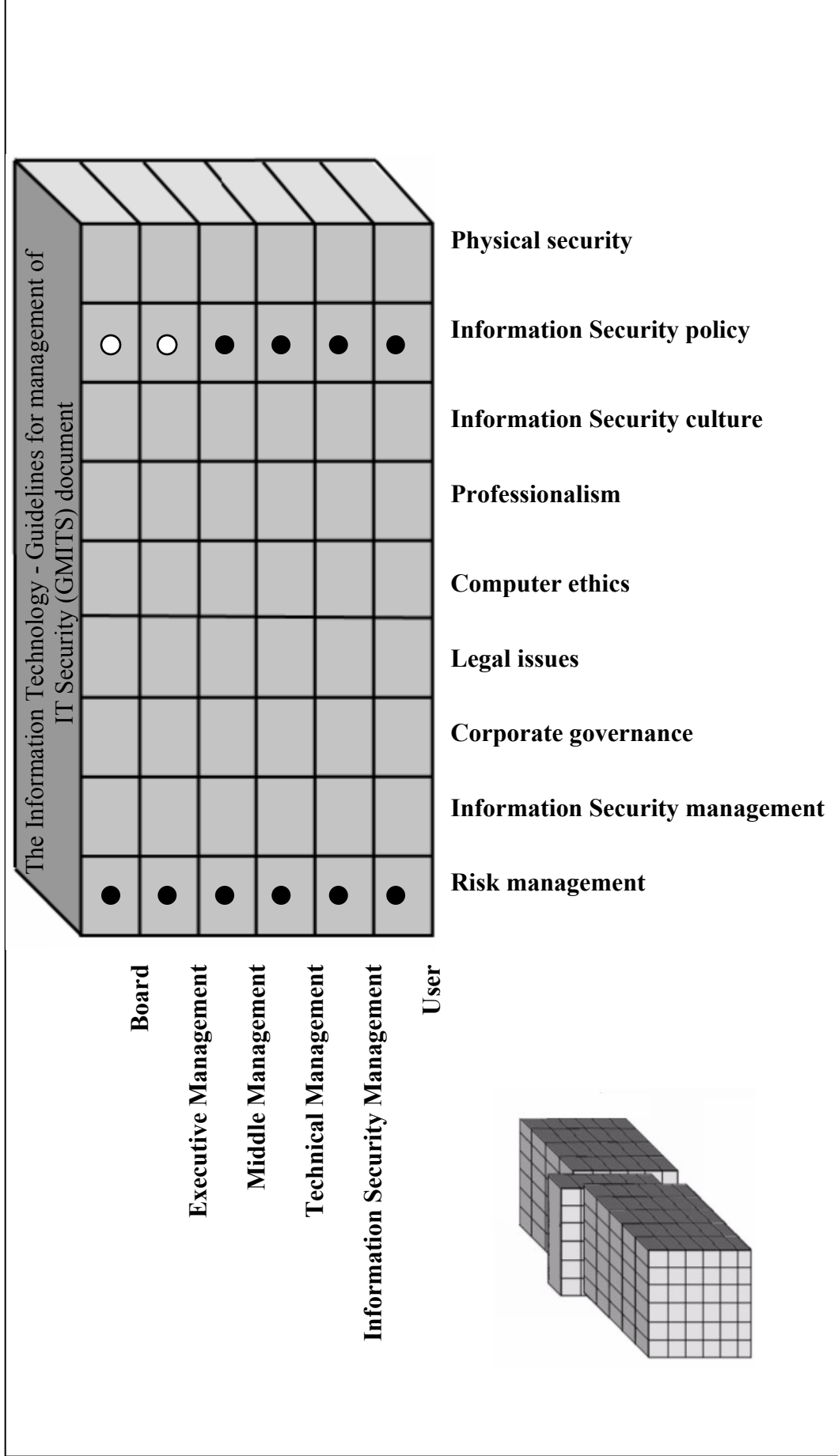


Figure 7.8: The Information Technology - Guidelines for Management of IT Security (GMITS) document

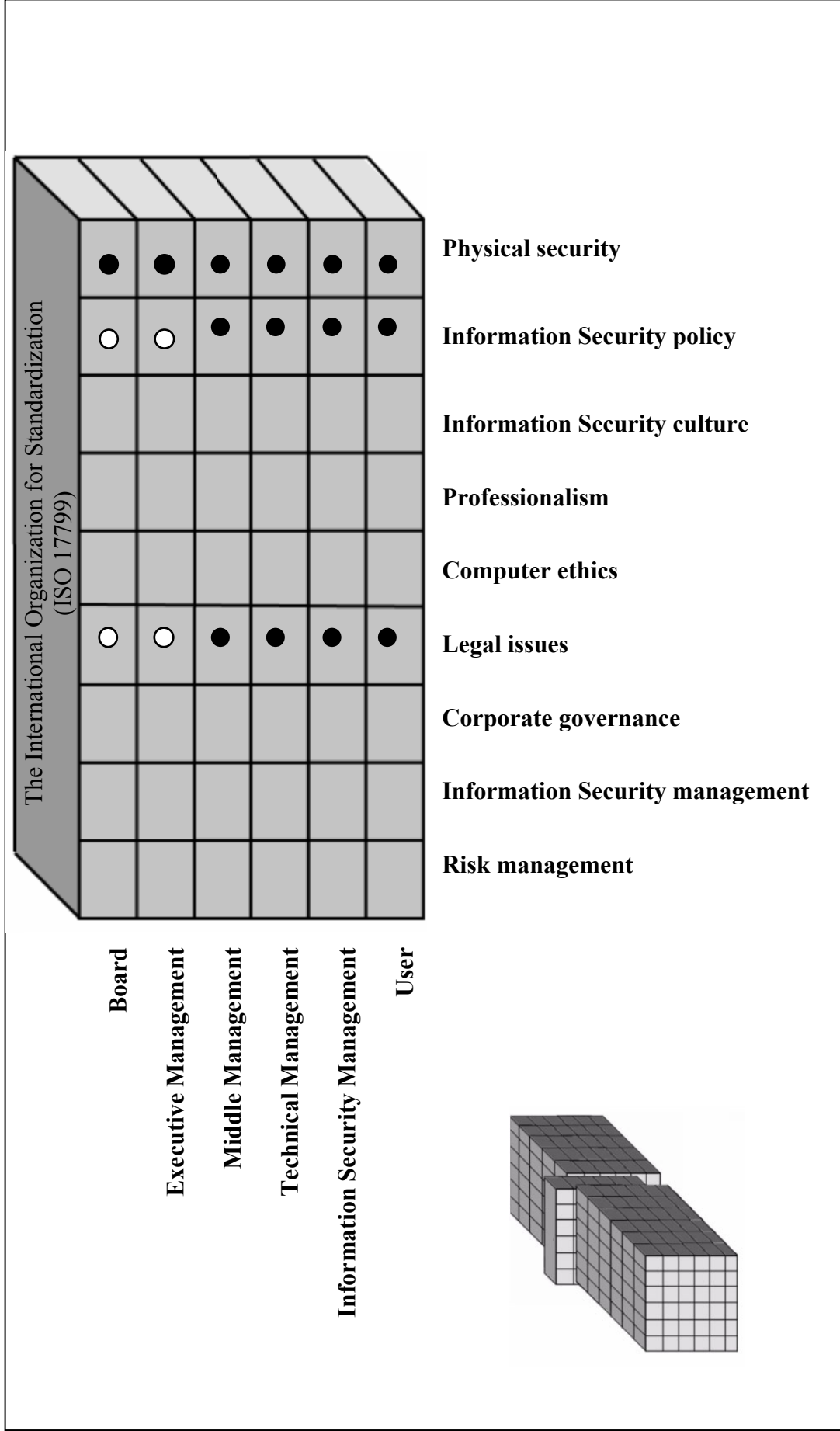


Figure 7.9: The International Organization for Standardization (ISO 17799)

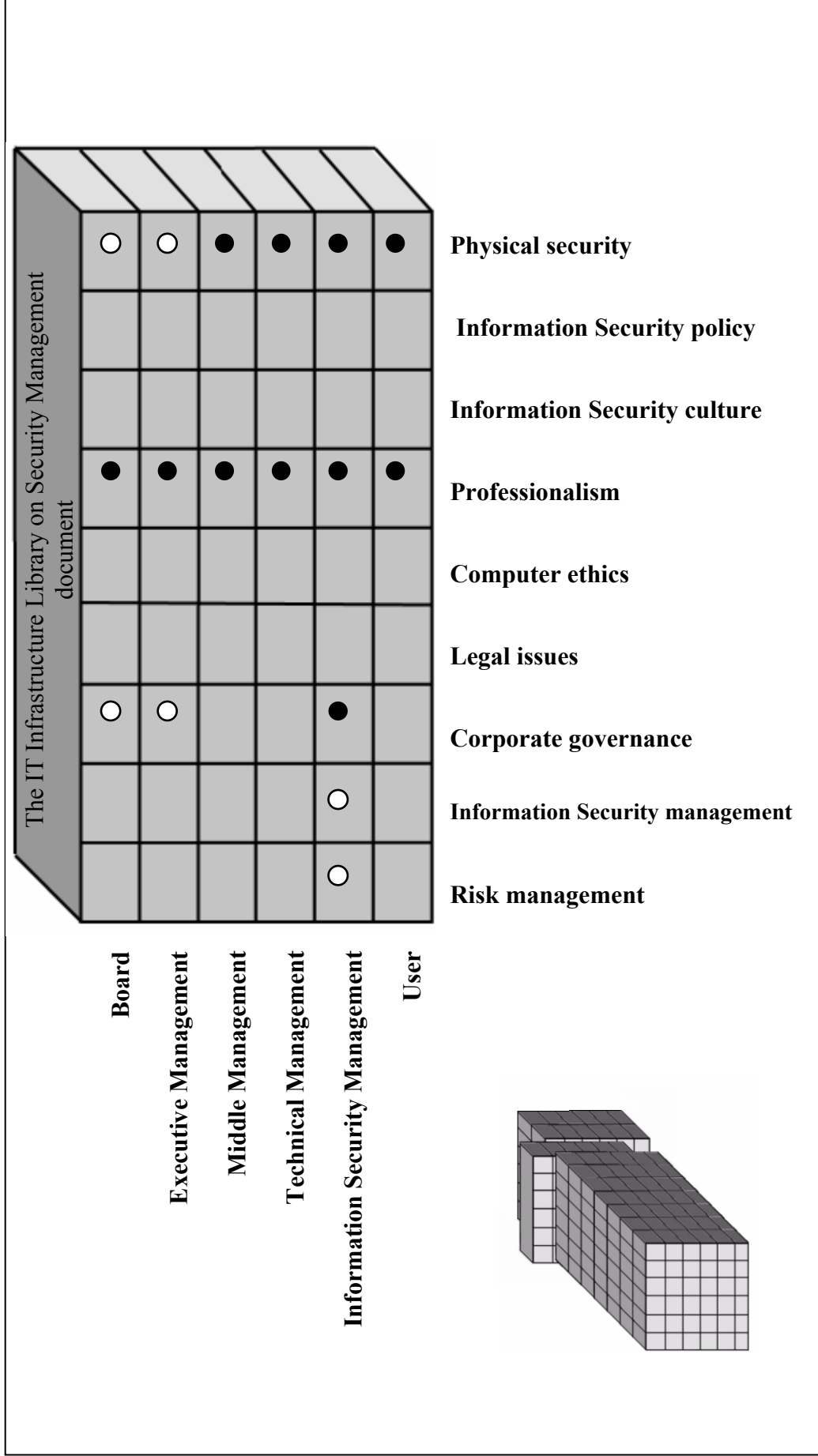


Figure 7.10: The IT Infrastructure Library on Security Management document

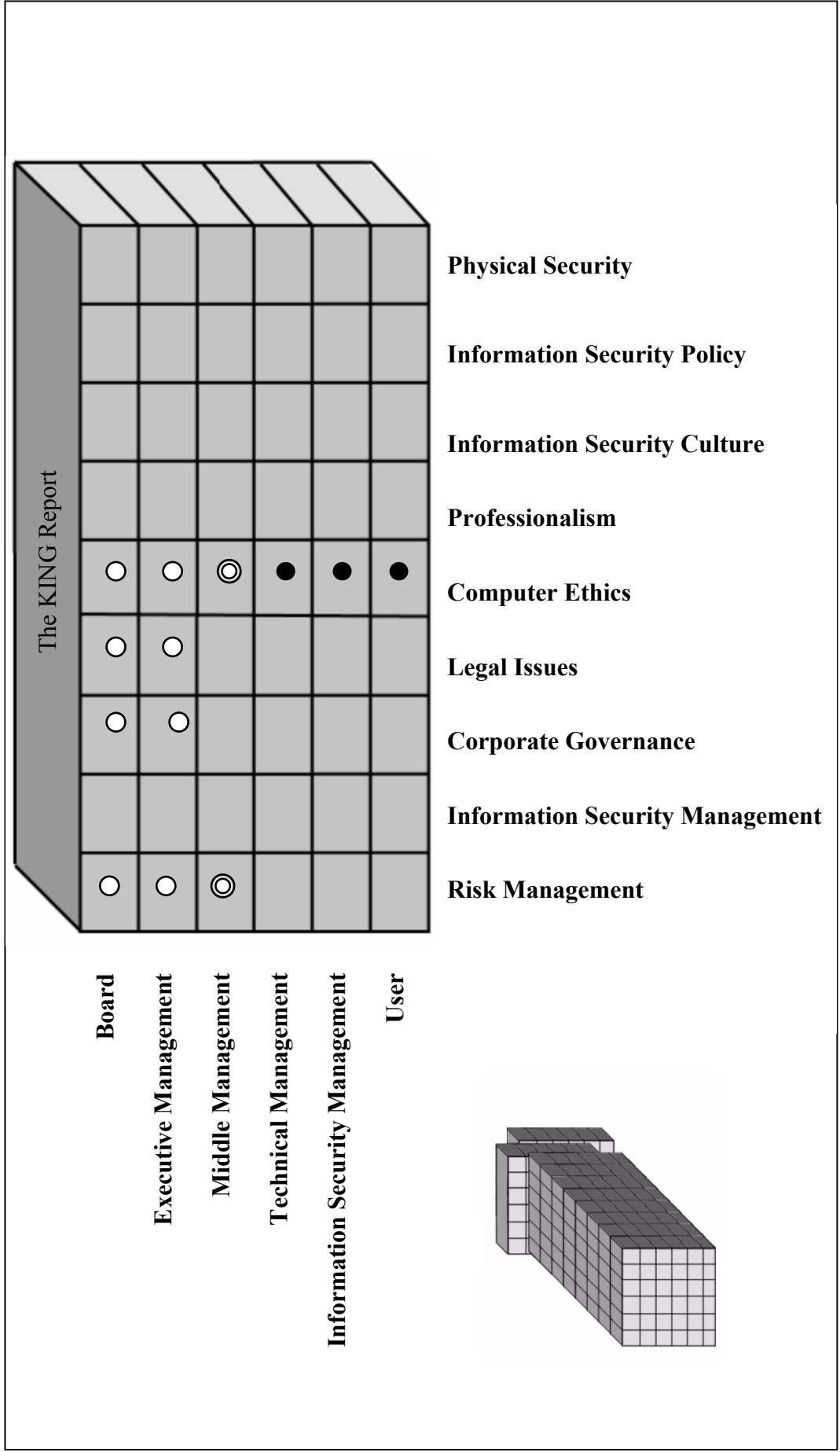


Figure 7.11: The KING report

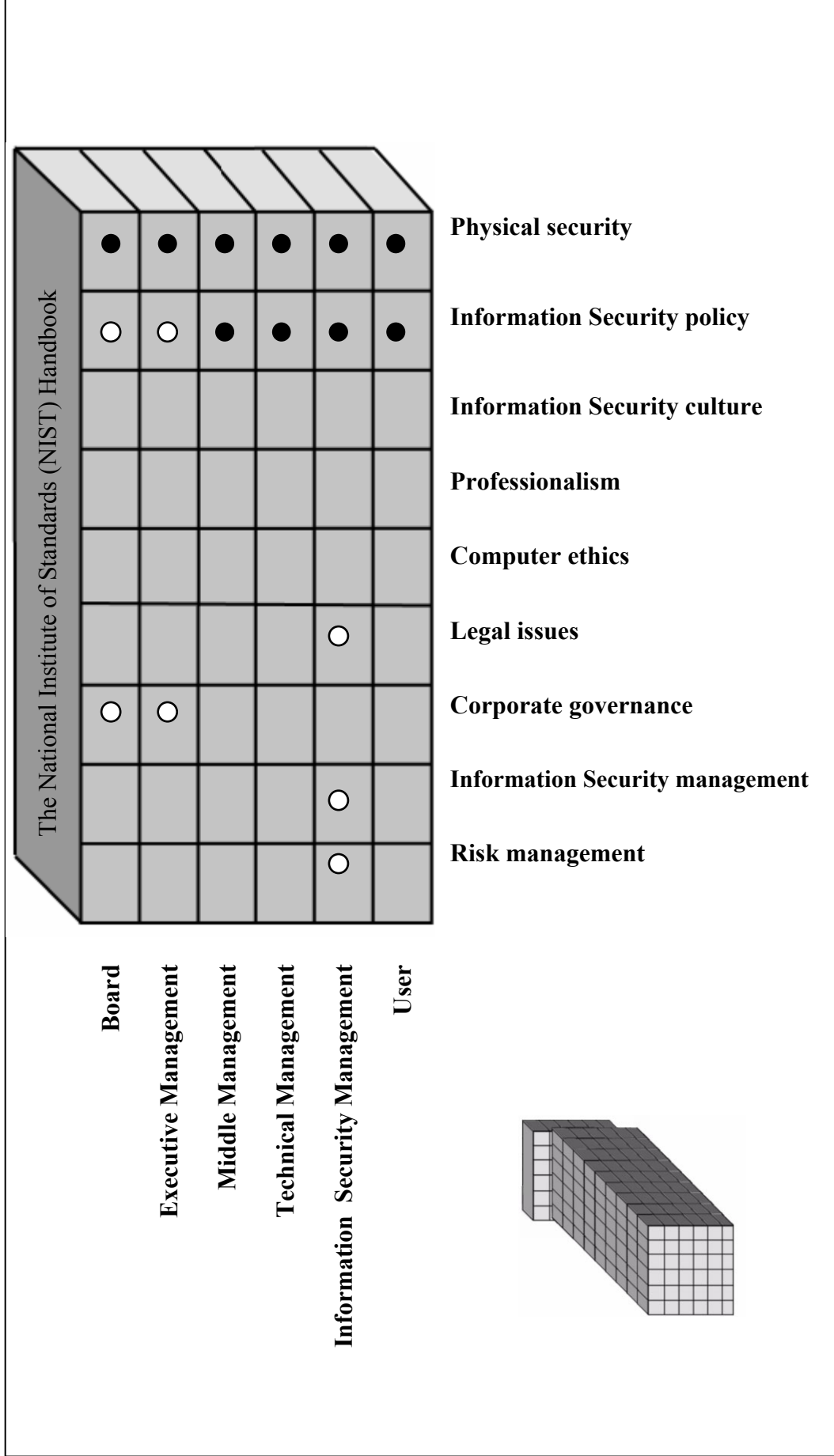
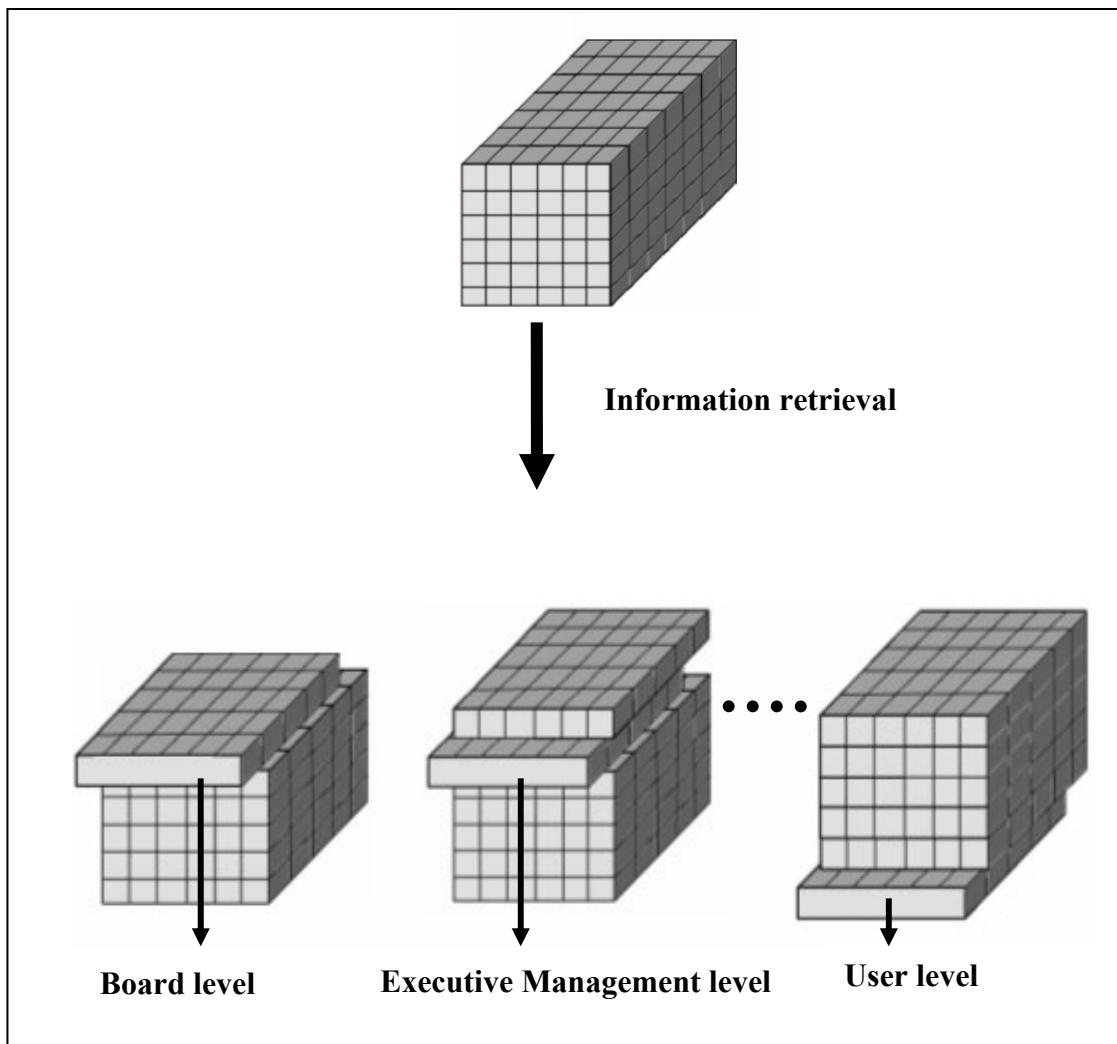


Figure 7.12: The National Institute of Standards (NIST) handbook



### 7.3.2 z-Slicing

The second slicing method will view the information in the ISRA Dimensions from the z-axis. The author refers to this slicing method as ‘z-slicing’. The z-slicing method enables stakeholders to extract information regarding individual **IT authority levels**. The z-slicing method is depicted in Figure 7.13.



*Figure 7.13: z-slicing*

In Figure 7.13 the dimensions are sliced to obtain relevant information regarding the specific non-technical Information Security issues that are highlighted within a specific Information Security document, for a specific IT authority level.

In the example depicted in Figure 7.13, the first horizontal slice represents the Board level. This slice includes the different non-technical Information Security issues

identified by the various Information Security documents relevant to the Board level. Similarly, the second slice represents the different non-technical Information Security issues identified by the various Information Security documents relevant to the Executive Management level, and so forth.

Figures 7.14 tot 7.19 show the relevant information that is obtained for each IT authority level by means of the z-slicing method. In these figures the ○ symbol is used for the IT authority level that is *ultimately responsible* for that specific non-technical Information Security issue according to a specific document. The ⊙ symbol is used for the IT authority level that should ensure that the *implementation* of a specific non-technical Information Security issue is completed according to a specific document. Lastly, the ● symbol indicates that a specific IT authority level should only be *aware* of that non-technical Information Security issue according to a specific document.

Consider Figure 7.14 as an example.

- According to the Board Briefing Document on IT Governance, the *Board* should be ultimately responsible for risk management and corporate governance.
- According to the Commonwealth Protection Manual, the *Board* level should be ultimately responsible for risk management, corporate governance Information Security policy and physical security, and be aware of legal issues.
- According to the Cadbury Report the *Board* level should be ultimately responsible for corporate governance and legal issues.
- According to COBIT the *Board* level should be ultimately responsible for risk management, corporate governance, legal issues, computer ethics, Information Security policy and physical security.
- According to the Information Security governance document, the *Board* level should be ultimately responsible for risk management, corporate governance and legal issues.
- According to the GMITS, the *Board* level should be aware of risk management and ultimately responsible for Information Security policy.

- According to the ISO 17799, the Board level should be ultimately responsible for legal issues and Information Security policy and be aware of physical security.
- According to the IT Infrastructure Library Document, the Board level should be ultimately responsible for corporate governance and physical security and be aware of professionalism.
- According to the King Report, the Board level should be ultimately responsible for risk management, corporate governance, legal and ethical issues.
- Finally, according to the NIST document the Board level should be ultimately responsible for corporate governance and Information Security policy and be aware of physical security.

The z-slicing method is applied to the remaining IT authority levels in a similar way as explained for the Board level. See Figures 7.15 to 7.19.

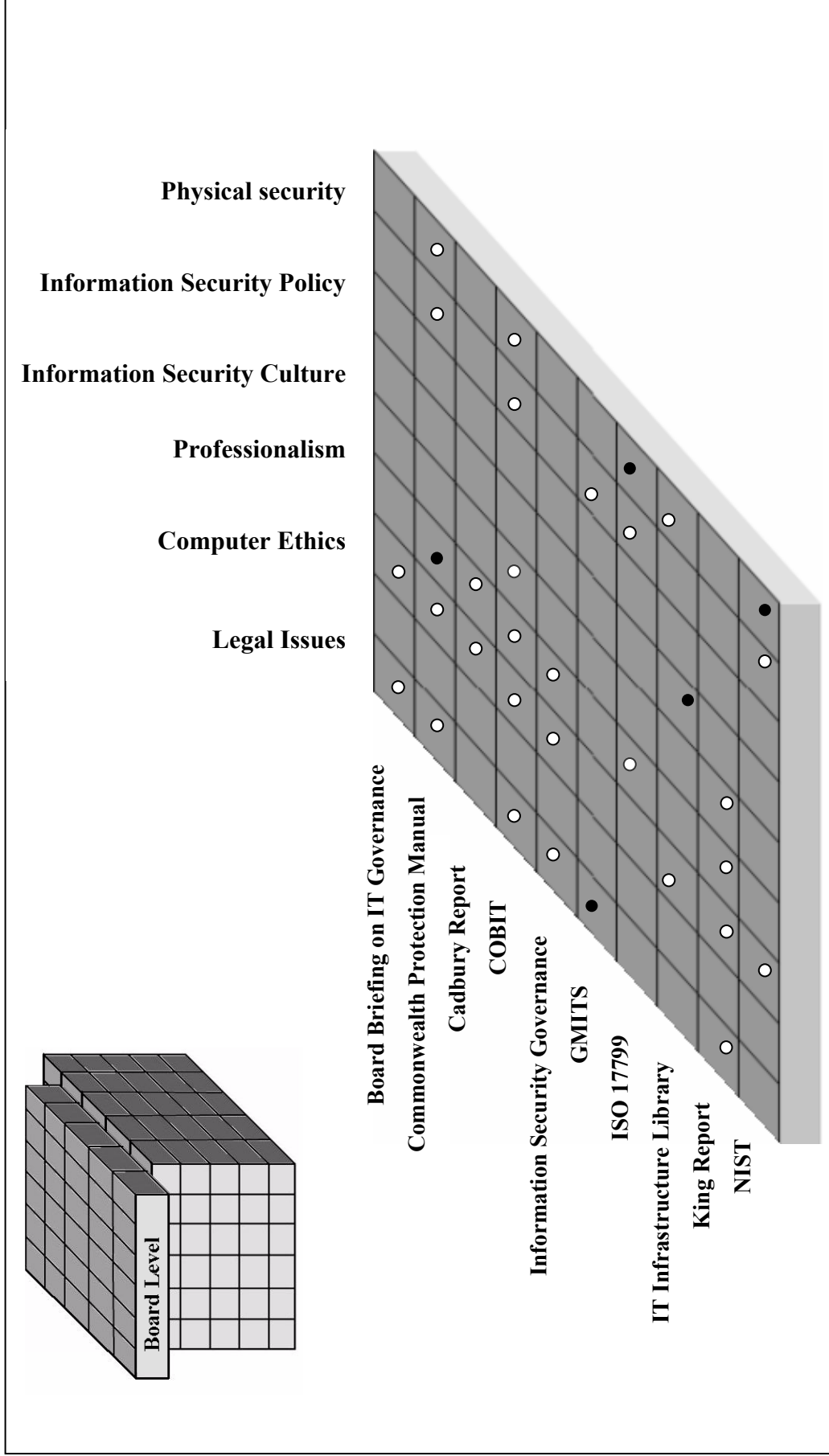


Figure 7.14: Board level

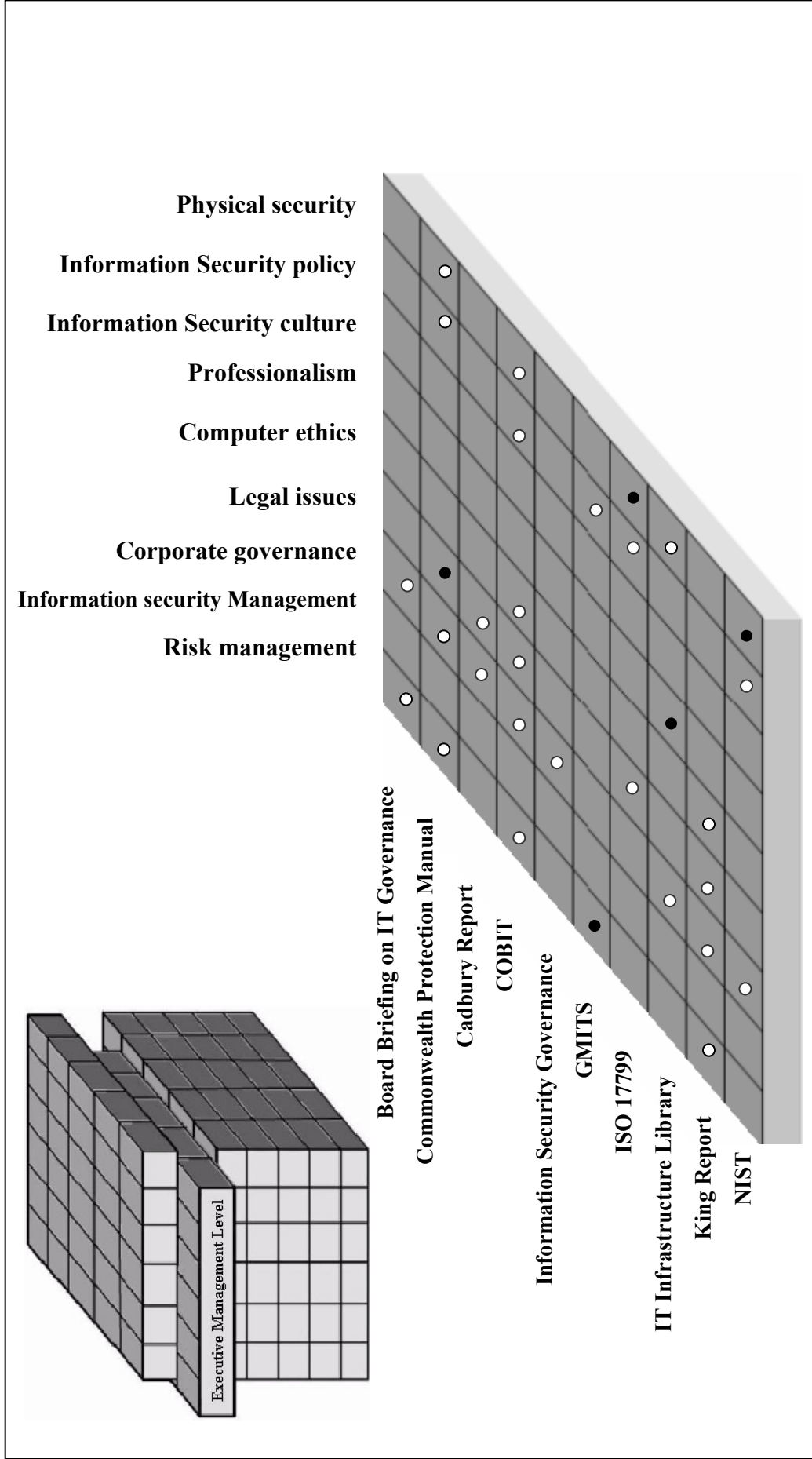


Figure 7.15: Executive Management level

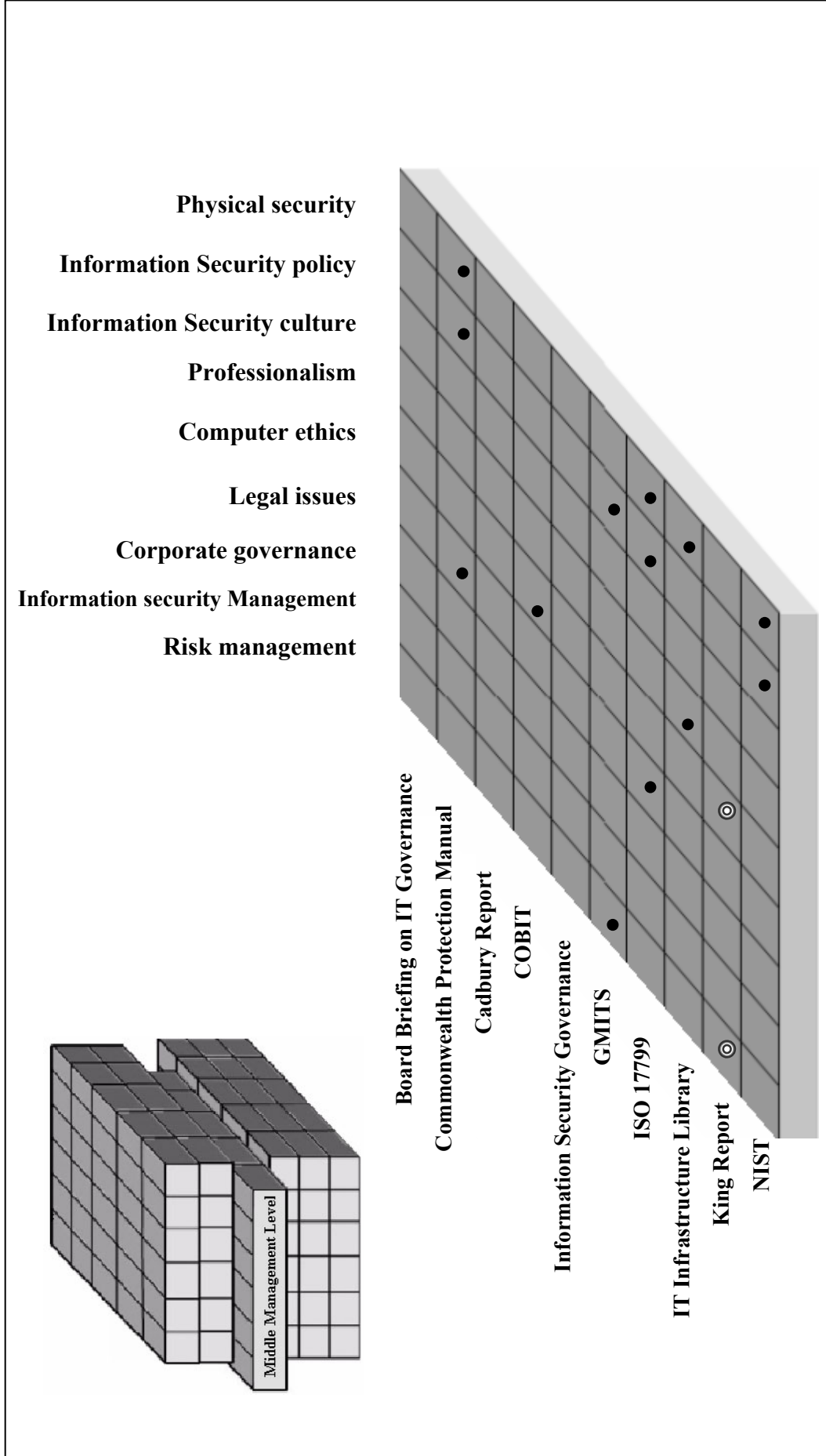


Figure 7.16: Middle Management level

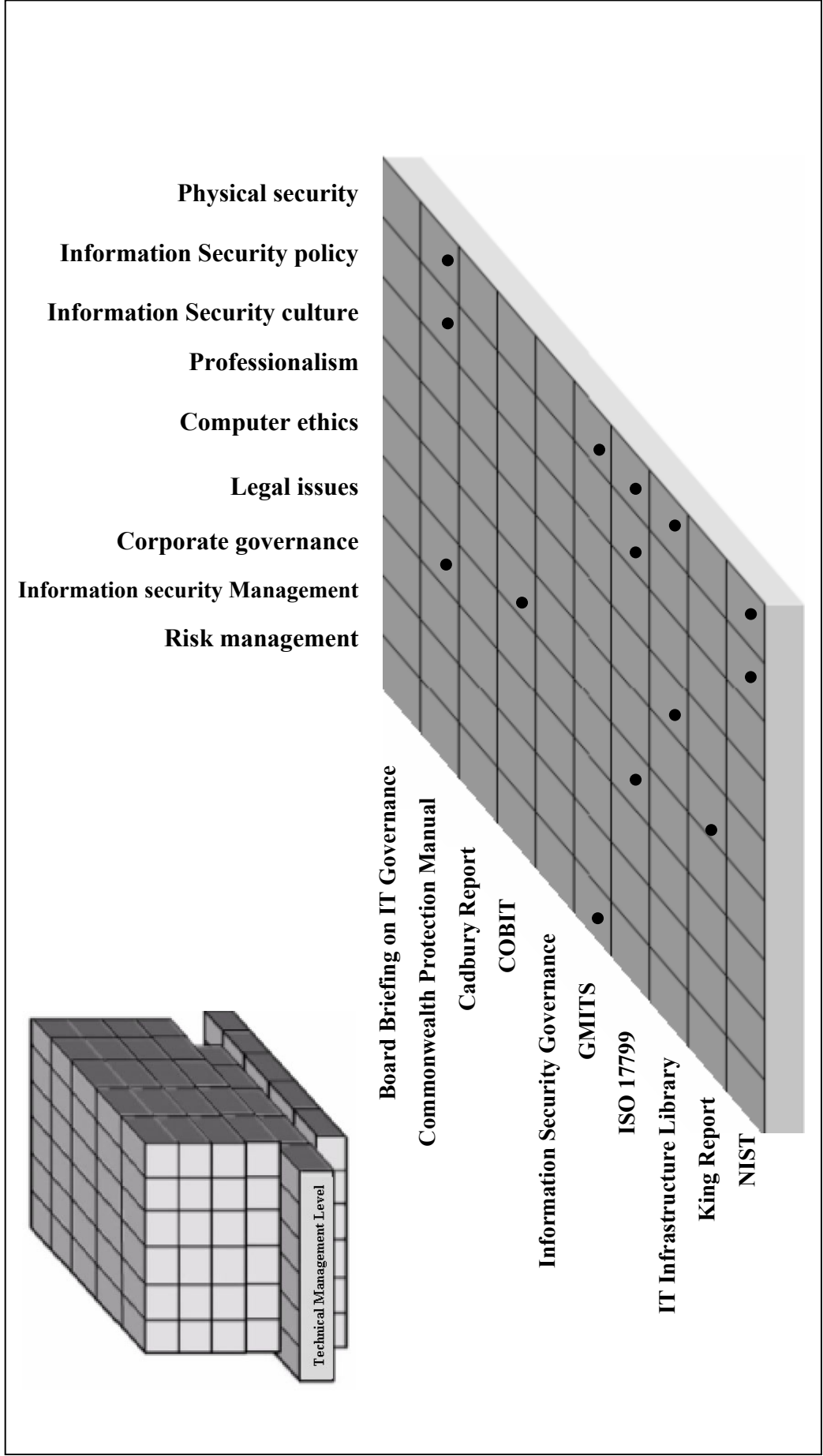


Figure 7.17: Technical Management level

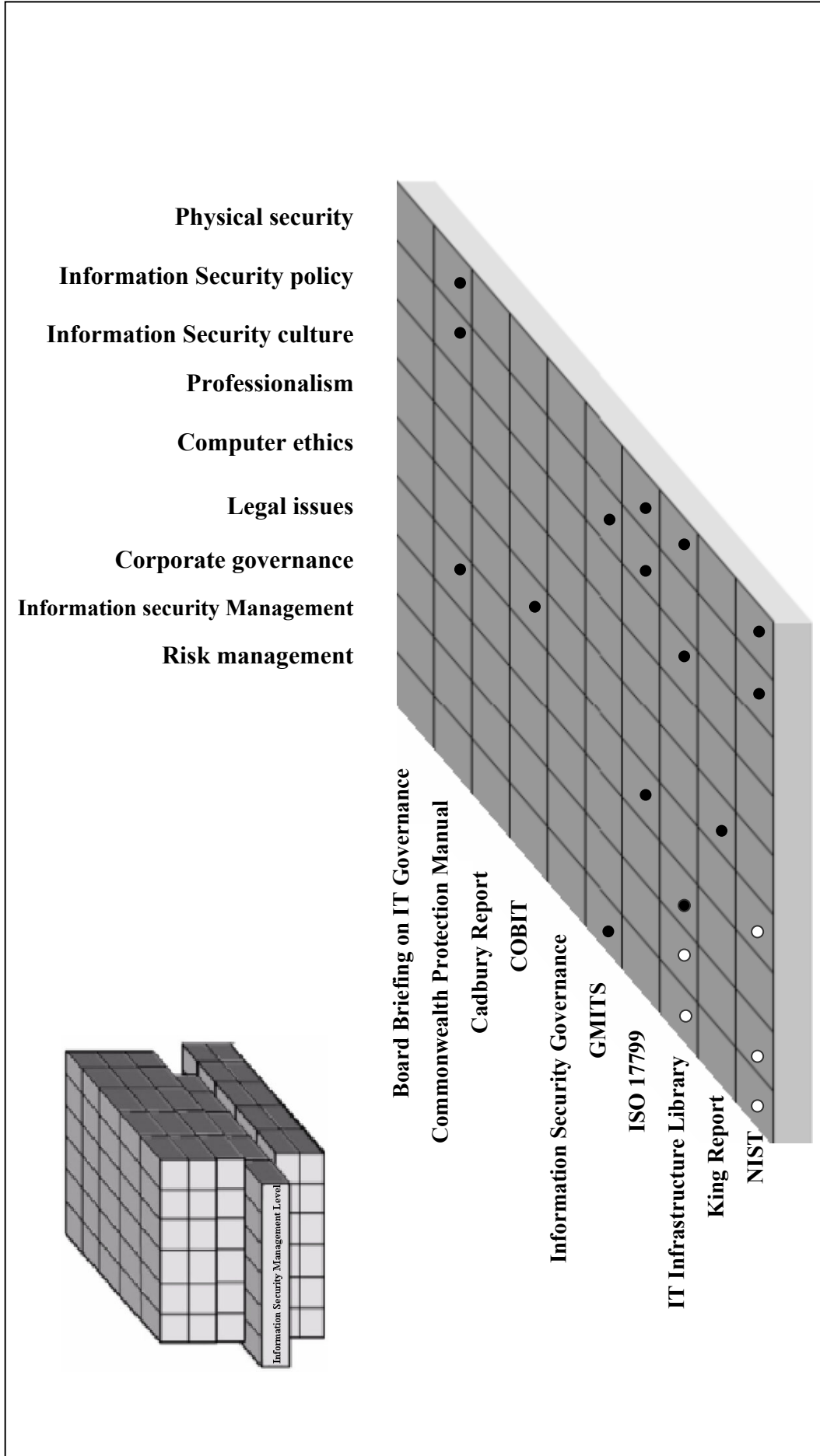


Figure 7.18: Information Security Management level



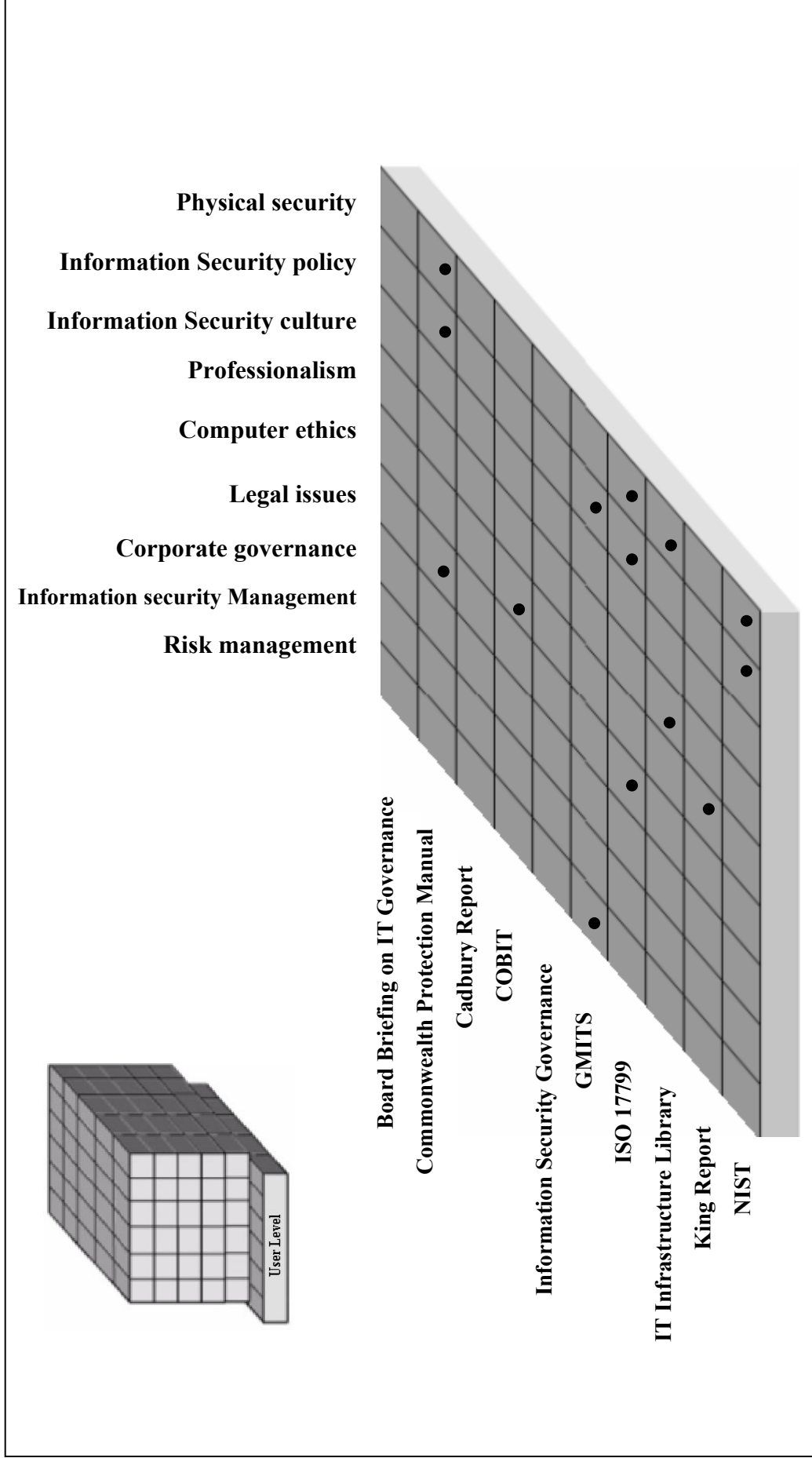
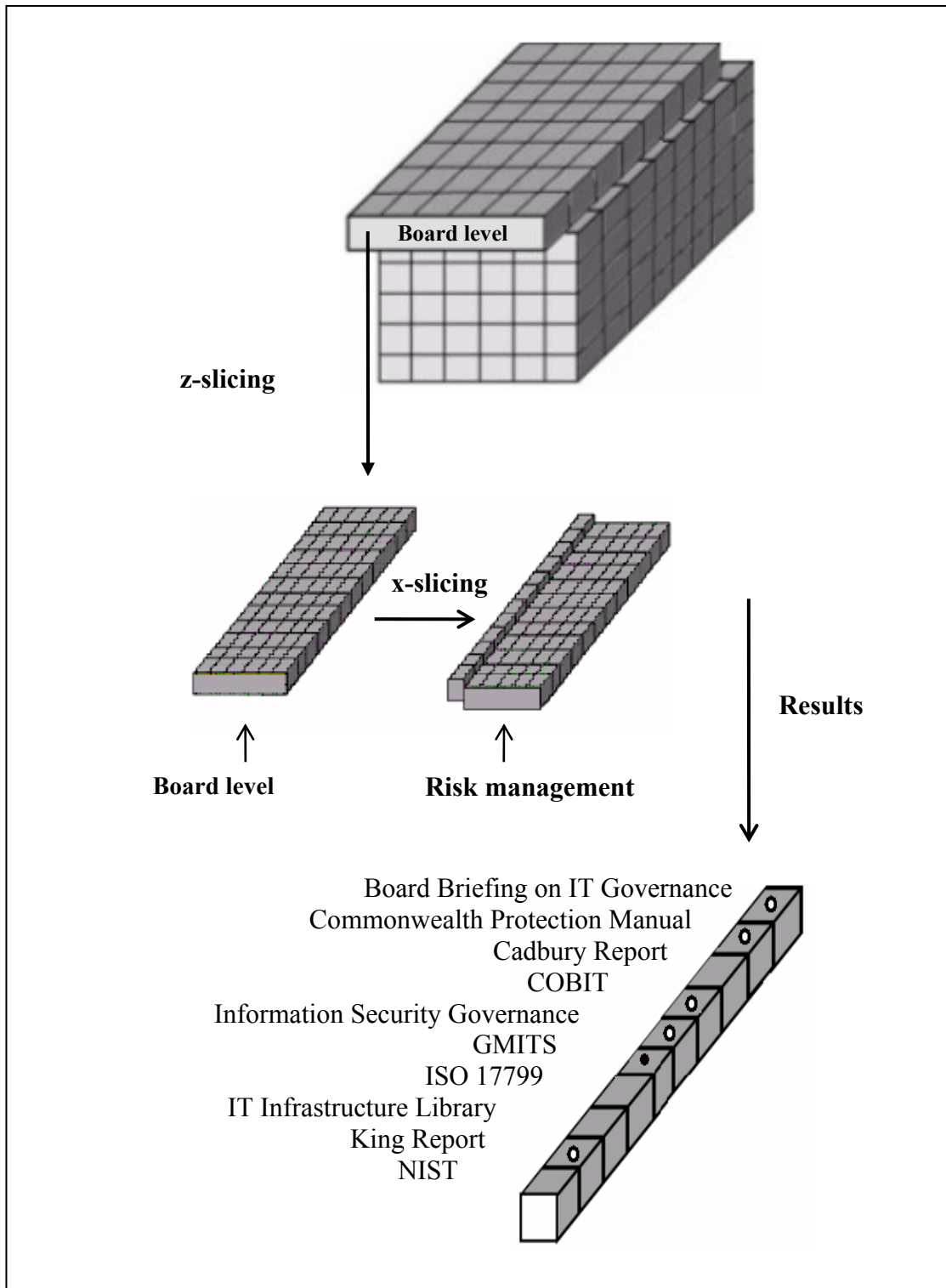


Figure 7.19: User level

### 7.3.3 Combination Slicing

The author refers to the third slicing method as the ‘combination-slicing method’, as it combines x-slicing, y-slicing and z-slicing in a specific sequence, depending on the request of the stakeholder. The x-slicing method is not discussed separately due to the fact that the information retrieved from this method is not very significant on its own. However, x-slicing is used within the combination-slicing method to enhance the y- and z-slicing methods. Therefore, the combination-slicing method is used when **detailed** information is required with regard to a specific IT authority level, non-technical Information Security issue and/or Information Security documents.

For example, consider a scenario where a stakeholder requests detailed information regarding the particular *Information Security documents that address risk management at Board level*. In this specific request, the sequence will be z-slicing followed by x-slicing (see Figure 7.20). To obtain the requested information, a z-slice is firstly taken to identify the Board level as the target IT authority level. Secondly, x-slicing is done on the z-slice that was obtained to identify risk management as the target non-technical Information Security issue. In Figure 7.20, the ○ symbol is used to indicate the IT authority level that is *ultimately responsible* for that specific non-technical Information Security issue according to a specific document. The ⊙ symbol is used to indicate the IT authority level that should ensure that the *implementation* of a specific non-technical Information Security issue is completed according to a specific document. Finally, the ● symbol indicates that a specific IT authority level should only be *aware* of that non-technical Information Security issue according to a specific document. The results in the example in Figure 7.20 therefore show that the Board level is ultimately responsible for risk management according to Board Briefing Document on IT Governance, Commonwealth Protection Manual, COBIT, Information Security Governance document and King Report. According to the GMITS document the Board level should only be aware of risk management.



**Figure 7.20: Results of the zx-slicing method**

Consider another scenario in which a stakeholder requests detailed information regarding the particular IT authority level that should be ultimately responsible for and/or ensure the implementation of and/or be aware of risk management according to the

Commonwealth Protective Security Manual. In this specific request the sequence will be y-slicing followed by x-slicing (see Figure 7.21).

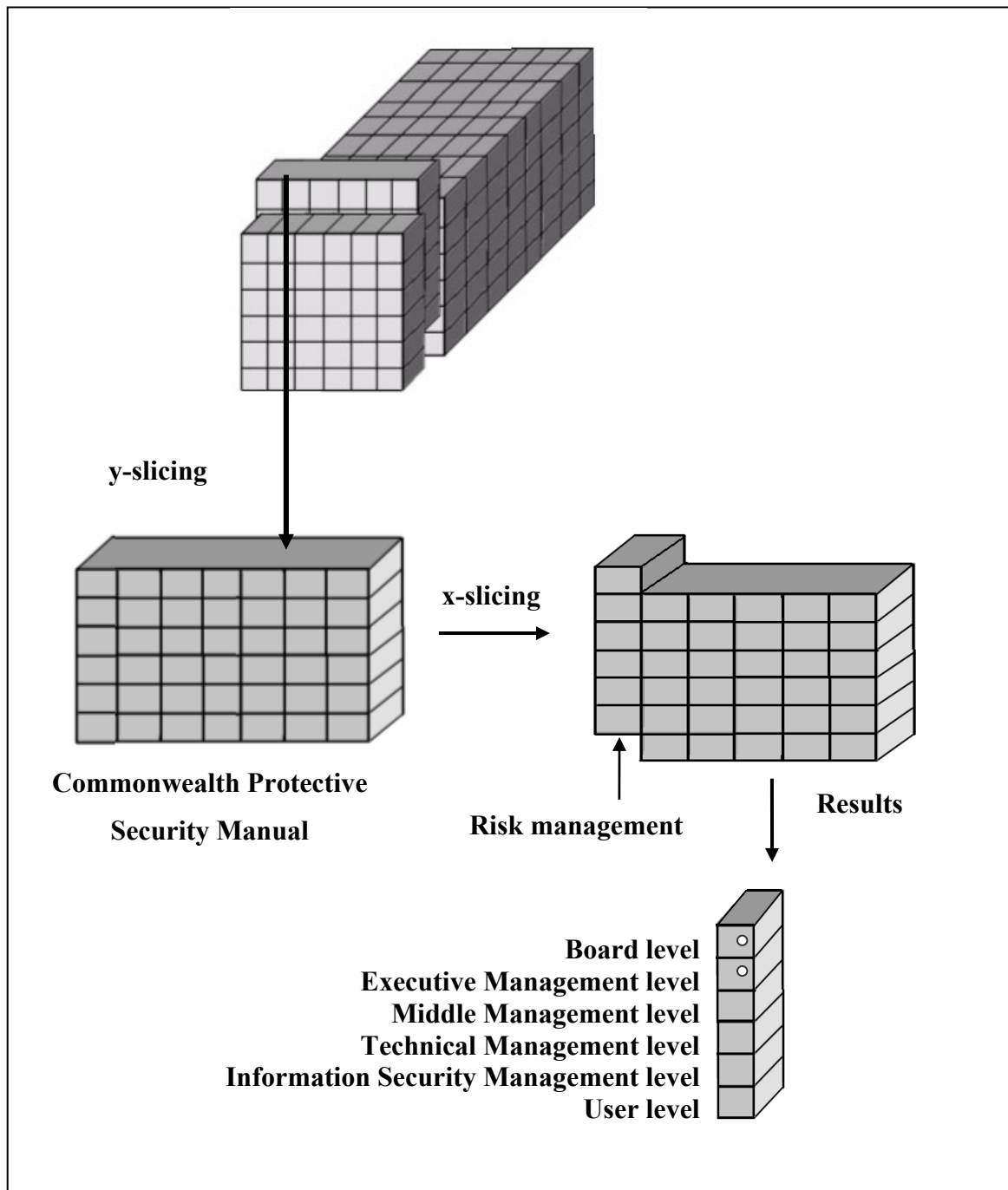


Figure 7.21: Results of the yx-slicing method

To obtain the requested information, a y-slice is firstly taken to identify the Commonwealth Protective Security Manual. Secondly, x-slicing is done on the y-slice obtained so as to identify risk management as the target non-technical Information Security issue. In Figure 7.21, the  $\circ$  symbol is used to indicate the IT authority level that

is *ultimately responsible* for that specific non-technical Information Security issue according to a specific document. The © symbol is used to indicate the IT authority level that should ensure that the *implementation* of a specific non-technical Information Security issue is completed according to a specific document. Finally, the ● symbol indicates that a specific IT authority level should only be *aware* of that non-technical Information Security issue according to a specific document. In Figure 7.21 the results show that according to the Commonwealth Protective Security Manual, the Board level and Executive Management level should be *ultimately responsible* for risk management.

There are various possibilities regarding requests for detailed information from the ISRA dimensions. All requests will be treated in a similar way by applying two of the three slicing methods (x-, y- and z-slicing) in a specific sequence based on the request.

### 7.4 Part 3: Measuring and Monitoring

The last part of the ISRA model focuses primarily on the measuring and monitoring of the current Information Security awareness status in an organisation. Measuring and monitoring the ISRA status in an organisation should be conducted regularly to ensure that the latest Information Security awareness status is known at any given time (Von Solms, 2001a).

The purpose of the *measuring process* is to determine the level of Information Security awareness of each stakeholder in the organisation with regard to all Information Security issues relevant to his/her IT authority level. Such level of awareness is measured on a scale ranging from 0 to 100% based on an Information Security awareness test that consists of a number of multiple choice questions related to a specific Information Security issue. These questions are based on the information contained in the Information Security documents that form part of the ISRA dimensions. The result of each test should be available immediately to indicate if there is a lack of knowledge regarding a specific Information Security issue. Each stakeholder must complete the relevant Information Security awareness test regularly to enhance his/her Information Security awareness and in this way ensure that human-related Information Security breaches are minimised.

The purpose of the *monitoring process* is to determine the Information Security awareness status within an organisation. The ISRA model also monitors this status by generating statistics based on the tests conducted during the measuring processes. These statistics are requested on an ad hoc basis by an IT authority level (such as the Board level) to determine if the organisation's Information Security awareness status is at an acceptable level and where problem areas lie. An example of a statistic that can be requested by the Board level is to display the percentage obtained for tests related to the latest Information Security policies. For each IT authority level, as well as for stakeholders within each IT authority level, the result of such a query will implicate the number of stakeholders who is still not participating in the Information Security awareness test.

The monitoring process should also ensure that new Information Security issues or documents are incorporated into the ISRA model as soon as possible.

### 7.5 Conclusion

This chapter provided an in-depth look at the three parts of the ISRA model.

The first part, the *ISRA Dimensions*, follows a three-dimensional approach by integrating state-of-the-art Information Security documents, IT authority levels and non-technical Information Security issues. Detailed information regarding these three dimensions was provided in Chapters 3, 4 and 5 respectively. The three dimensions constitute the building blocks of the ISRA model and will be used as the basis for the second part.

The second part of the ISRA model concerns *Information Security Retrieval and Awareness* and focuses on retrieving information from the ISRA dimensions. Three slicing methods (y, z and combination slicing) were introduced that could assist IT authority levels to extract relevant information directly from the ISRA dimensions without involving a third party. This does not only save time and effort, but also ensures that stakeholders are not burdened with irrelevant information.

The third part of the ISRA model involves *Measuring and Monitoring*. It aims to measure the level of Information Security awareness of each stakeholder in an organisation.

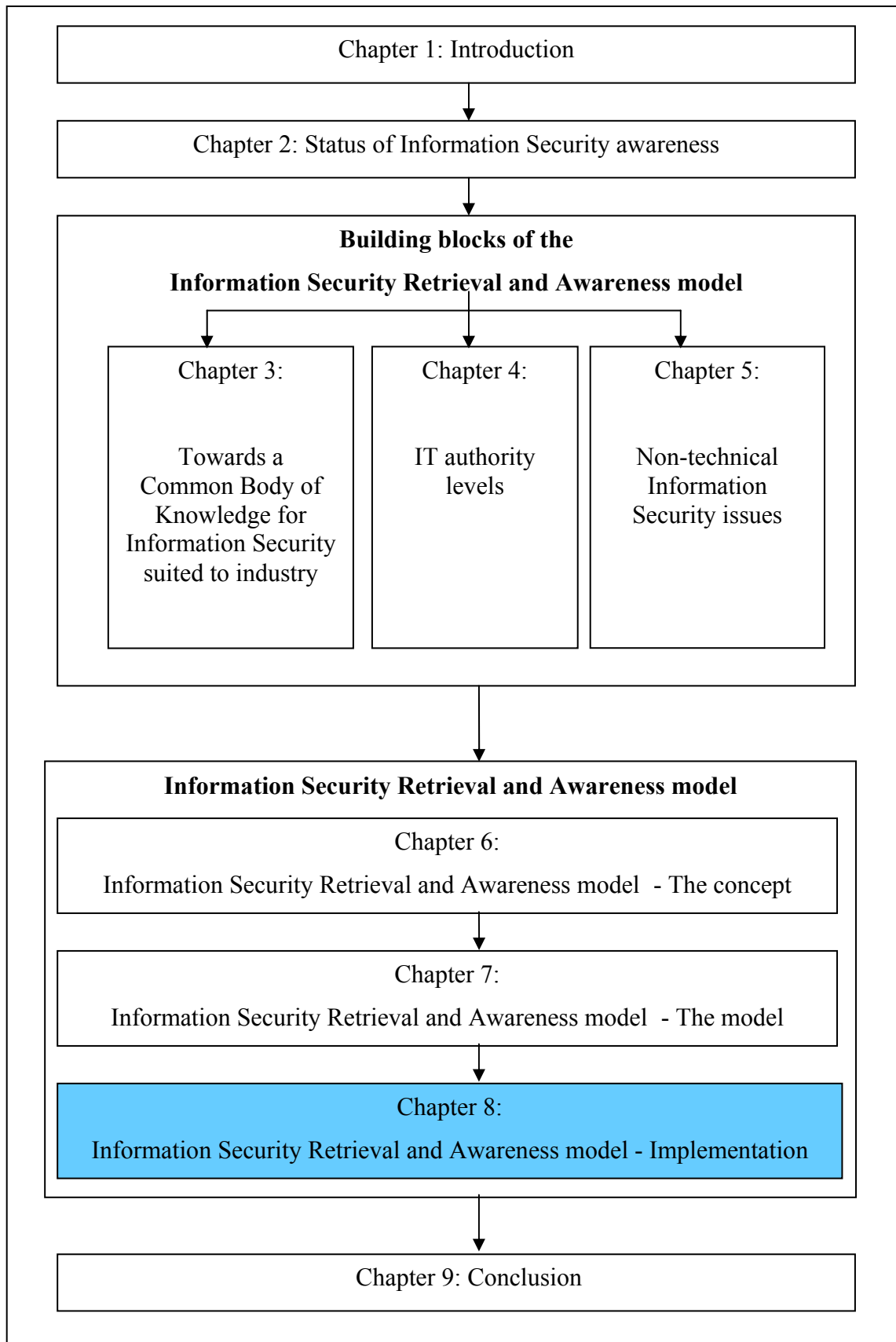
Additionally, it aims to monitor the Information Security awareness status of an organisation with a view to identifying problem areas.

The next chapter, Chapter 8, will be devoted to a discussion of the implementation of the ISRA model.

## **Chapter 8**

# **Information Security Retrieval and Awareness (ISRA) model – Implementation**





### 8.1 Introduction

The purpose of this chapter is to illustrate that the Information Security Retrieval and Awareness (ISRA) model is not merely a theoretical concept, but that it can indeed be implemented successfully. The chapter is devoted to a discussion of the prototype developed to illustrate the functioning of the ISRA model. The prototype is used to achieve the main objective of the ISRA model, namely to enhance Information Security awareness among employees.

The prototype was developed by a South African company, IT Event Management, on a Pentium 4 MHZ computer in a Windows 2003 environment using Visual Basic 6 and JavaScript. The specifications for the prototype that the author presented to IT Event Management are supplied in Appendix A of this thesis. The prototype can be found at the following URL: <http://www.it-em.ac.za/isra>. Instructions for executing the prototype are supplied in Appendix B of this thesis.

### 8.2 Scope of the prototype

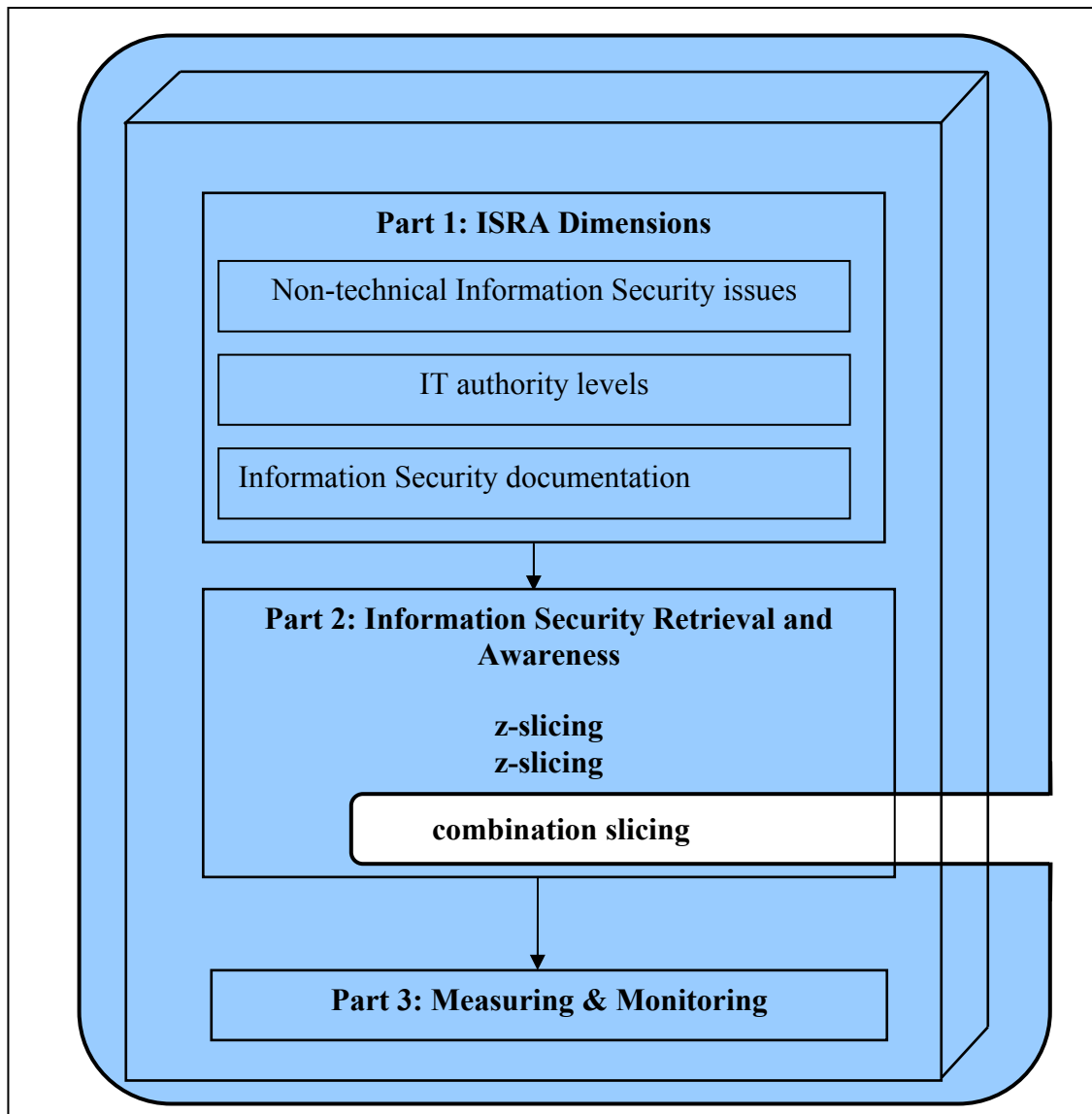
The prototype implements all three parts of the ISRA model (i.e. Information Security Dimensions, Information Security Retrieval and Awareness, and Measuring and Monitoring).

The first part of the ISRA model was implemented by the author by populating the database with information regarding the different IT authority levels, non-technical Information Security issues and state-of-the-art Information Security documents. This function will typically be performed by the Information Security Manager. The structure of the database is provided in Appendix A of this thesis as part of the specifications.

The second part of the ISRA model deals with Information Security Retrieval and Awareness. The Information Security Awareness part is implemented by incorporating on-line Information Security awareness tests. The Information Security *Retrieval* part, on the other hand, provides the user with the functionality of retrieving relevant information regarding Information Security issues from the database, at any time and without involving a third party. The prototype incorporates the y- and z- slicing retrieval methods only.

Finally, the last part of the ISRA model (Measuring and Monitoring) provides management with the opportunity to *measure* the Information Security awareness of employees at any time, as well as to *monitor* the Information Security awareness status in the organisation.

The scope of the prototype is depicted by the shaded area in Figure 8.1.

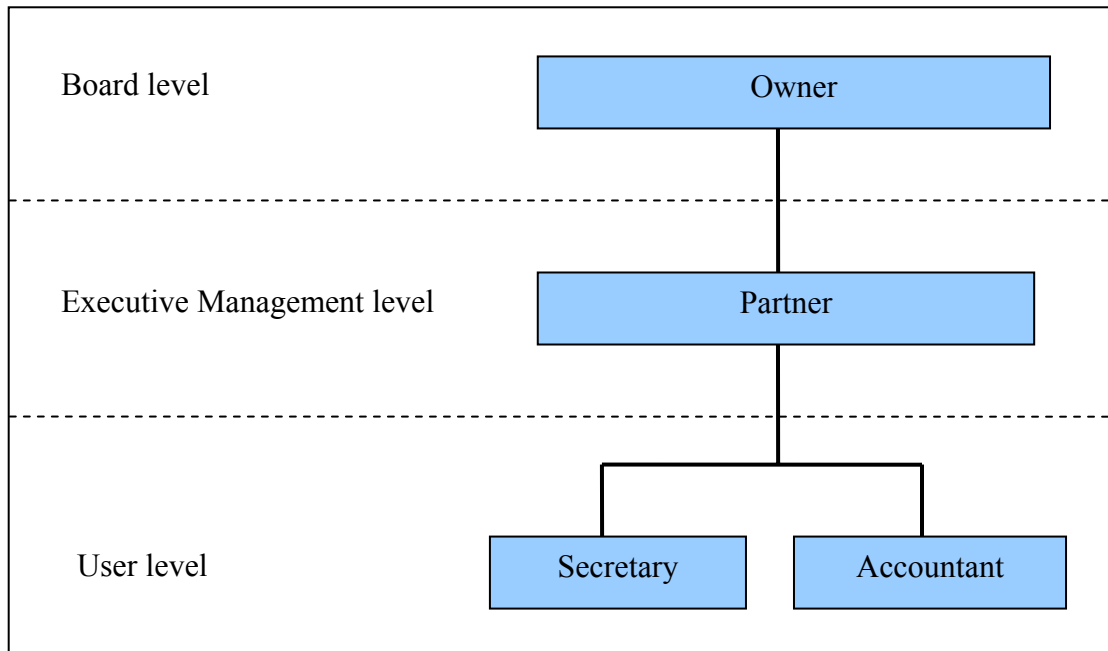


*Figure 8.1: Scope of prototype*

The purpose of this chapter is to demonstrate the implementation of the ISRA model and it should therefore not be seen as a user's guide for executing the prototype (the user's guide is presented in Appendix B of this thesis).

### 8.3 Real-life industry-based organisation

The prototype was implemented in a small real-life industry-based organisation in South Africa - *Bekker & du Toit Optometrists*<sup>1</sup>. Figure 8.2 depicts the organisational structure of Bekker & du Toit Optometrists.



*Figure 8.2: Organisational structure of Bekker & du Toit Optometrists*

Bekker & du Toit Optometrists consists of four stakeholders (i.e. owner, partner, secretary and an accountant). These stakeholders are grouped into three IT authority levels namely, Board level, Executive Management level and User level.

Bekker & du Toit Optometrists outsource their Information Security functions, such as making backups, adding and deleting information regarding employees from the database and updating the anti-virus program. They therefore do not have an Information Security Management level as part of their IT authority levels. The author performed all the functions of an Information Security Manager for the purpose of implementing the prototype.

Since all stakeholders in this organisation have access to sensitive information on a daily

---

<sup>1</sup> Permission was obtained to include the company's name in this thesis.

basis, they expressed a need for a system that will enhance the Information Security awareness among all stakeholders in order to minimise the occurrence of human-related Information Security breaches. All stakeholders participated in the implementation phase of the prototype.

Bekker & du Toit Optometrists identified the following non-technical Information Security issues as currently being essential to their organisation:

- Computer ethics
- Physical security
- Corporate governance (including Information Security governance)
- Security policies

For the purpose of testing the prototype, the author had to populate the database. As mentioned earlier, this function used to be outsourced. Based on the need specified by Bekker & du Toit Optometrists, the focus of the implementation was on the non-technical Information Security issues mentioned above and on the three IT authority levels - as depicted in Figure 8.2.

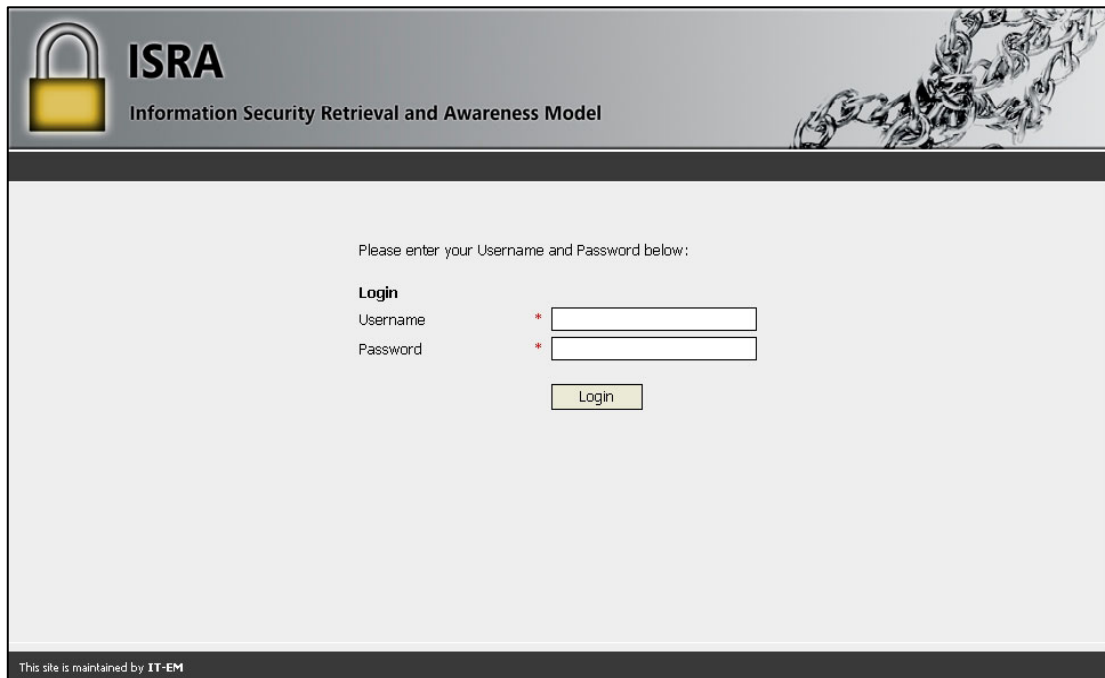
In addition, the owner required the following statistical information:

- The results of the Information Security awareness tests for each stakeholder.
- The Information Security risk areas in the organisation.

### **8.4 The prototype**

The functioning of the prototype will subsequently be discussed based on the actions performed by each stakeholder when the prototype was used.

When the prototype is loaded, it presents the user with the Login screen as depicted in Figure 8.3.



ISRA  
Information Security Retrieval and Awareness Model

Please enter your Username and Password below:

**Login**

Username \*

Password \*

This site is maintained by IT-EM

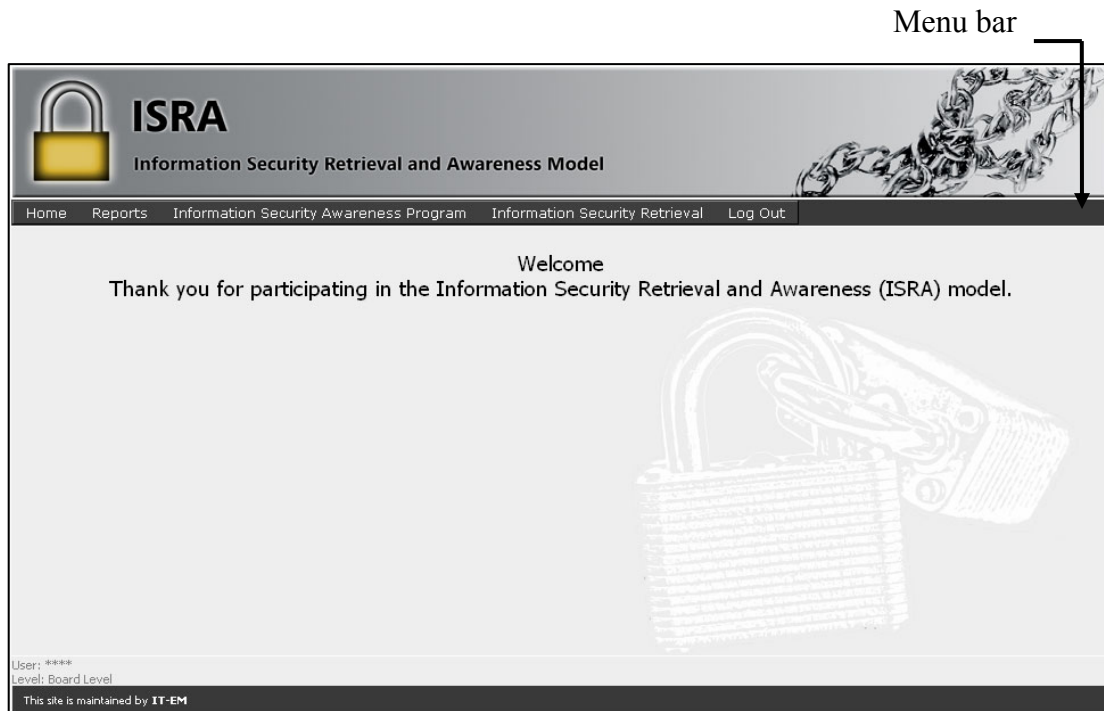
*Figure 8.3: Login screen*

All users of the system will be provided with a Username and Password by the author due to the fact that the security functions have previously been outsourced. All passwords are saved in an encrypted format in the database to enhance the security of the system. In the Login process it is compulsory that the Username and Password combination be provided correctly before access to the system is granted. If the user provides an *incorrect* Password or Username, the system will display an error message.

### **8.4.1 Information Security Awareness Program**

#### **8.4.1.1 Board level**

The Board level of Bekker & du Toit Optometrists consists of one stakeholder, namely the owner. Figure 8.4 depicts the different menu options on the menu bar available to the owner after having logged in successfully.



***Figure 8.4: Home screen for Board level***

Note that the Username displayed at the bottom of the screen has been disguised by using the \* symbol to protect the identity of the user. The IT authority level<sup>2</sup> of the current user is displayed below the disguised Username. The first option selected by the owner was the Information Security Awareness Program option on the menu bar, and the screen that is displayed as a result is depicted in Figure 8.5.

---

<sup>2</sup> For the purpose of this thesis the database was populated with only the three IT authority levels that are represented in Bekker & Du Toit Optometrists (see Figure 8.2) – as well as with the Information Security Manager.

Information Security Issues relevant to your IT Authority Level		Date & Result of last test
<a href="#">Computer Ethics</a>	<a href="#">Do Test</a>	No Result
<a href="#">Corporate Governance</a>	<a href="#">Do Test</a>	No Result
<a href="#">Physical Security</a>	<a href="#">Do Test</a>	No Result
<a href="#">Security Policy</a>	<a href="#">Do Test</a>	No Result

Back

User: \*\*\*\*  
Level: Board Level  
This site is maintained by IT-EM

*Figure 8.5: Information Security Awareness Program screen*

This screen lists all the non-technical Information Security issues<sup>3</sup> relevant to the Board level, with links to access information related to a specific Information Security issue (with a view towards preparing for a test). Additionally, links to complete an Information Security awareness test for each issue are also provided. The screen furthermore displays the date and the result (0%-100%) of the last completed test – currently no tests have been completed by the owner.

The owner first viewed information on each of the non-technical Information Security issues listed by clicking on the appropriate link. Figures 8.6 to 8.9 depict the screens displayed when the owner clicked on the Computer Ethics, Corporate Governance, Physical Security and Security Policy links respectively.

<sup>3</sup> For the purpose of this thesis the database was populated with only the four Information Security issues identified by Bekker & du Toit Optometrists (as mentioned in paragraph 8.3).



**ISRA**  
Information Security Retrieval and Awareness Model

Home Reports Information Security Awareness Program Information Security Retrieval Log Out

**The KING report**

- Establish the values of the enterprise in support of its vision and mission
- Establish principles and standards of ethical business practice for the enterprise in support of such values
- Ensure communication of established principles and standards to affected stakeholders in codified form
- Assume responsibility and accountability to stakeholders for compliance with such principles and standards.
- Effective communication of its strategic plans and ethical code both internally and externally.

**Governance, Control and Audit for Information and Related Technology (COBIT)**

Management should create a framework and an awareness programme fostering a positive control environment throughout the entire organisation by addressing aspects such as: integrity, **ethical values** and competence of the people; management philosophy and operating style; and accountability, attention and direction provided by the board of directors.

Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the policies and procedures are being followed. Compliance procedures for **ethical**, security and internal control standards should be set by top management and promoted by example.

All personnel should be trained and educated in system security principles. Senior management should provide an education and training programme that includes: ethical conduct of the information services function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.

**Governance, Control and Audit for Information and Related Technology (COBIT)**

Management should create a framework and an awareness programme fostering a positive control environment throughout the entire organisation by addressing aspects such as: integrity, **ethical values** and competence of the people; management philosophy and operating style; and accountability, attention and direction provided by the board of directors.

Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the policies and procedures are being followed. Compliance procedures for **ethical**, security and internal control standards should be set by top management and promoted by example.

All personnel should be trained and educated in system security principles. Senior management should provide an education and training programme that includes: ethical conduct of the information services function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.

**Commonwealth Protective Security Manual**

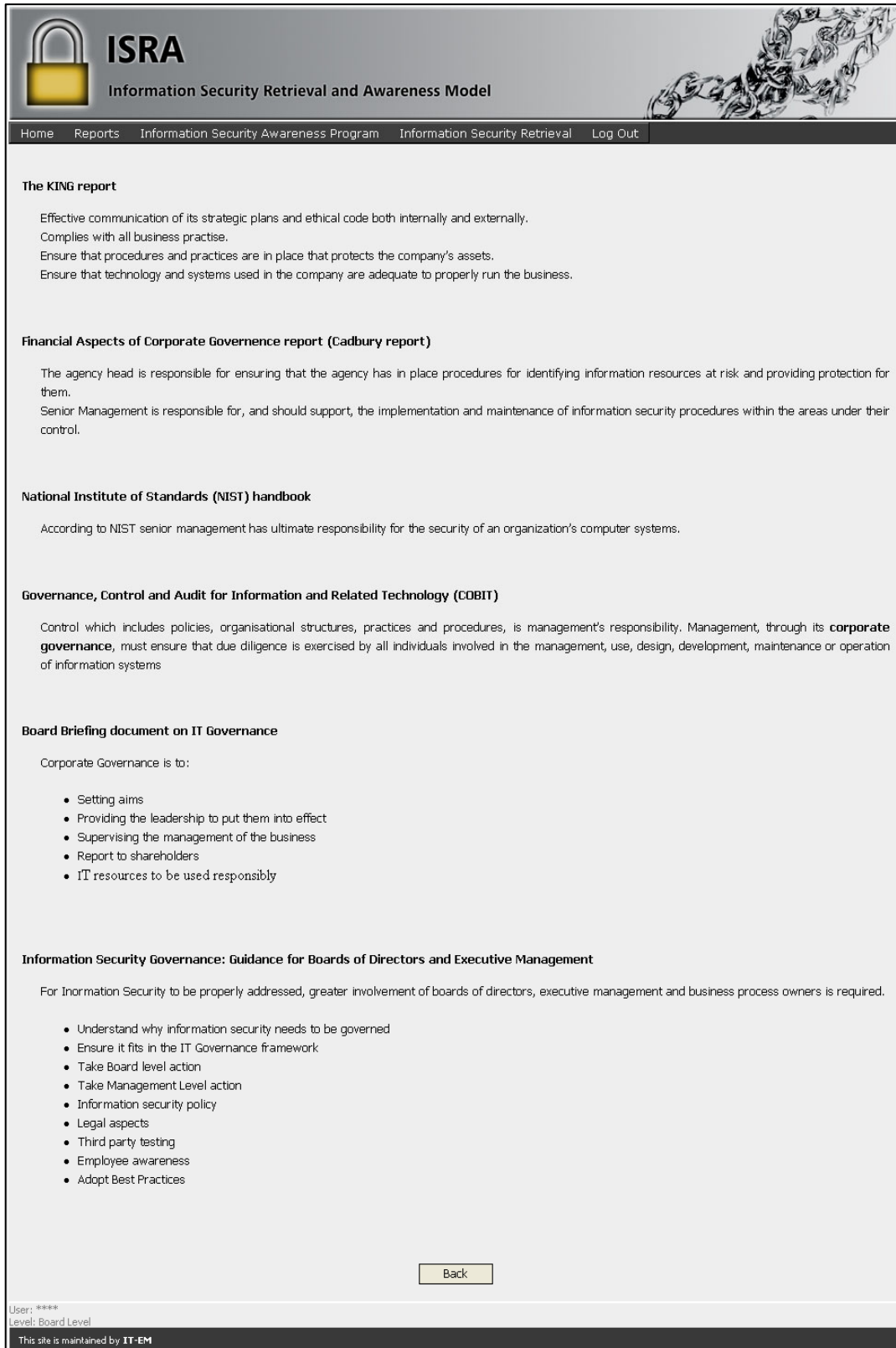
The agency head is responsible for ensuring that the agency has in place procedures for identifying information resources at risk and providing protection for them.

Senior Management is responsible for, and should support, the implementation and maintenance of information security procedures within the areas under their control.

[Back](#)

User: \*\*\*\*  
Level: Board Level  
This site is maintained by IT-EM

*Figure 8.6: Detailed information on computer ethics*



**ISRA**  
Information Security Retrieval and Awareness Model

Home Reports Information Security Awareness Program Information Security Retrieval Log Out

**The KING report**

Effective communication of its strategic plans and ethical code both internally and externally.  
Complies with all business practise.  
Ensure that procedures and practices are in place that protects the company's assets.  
Ensure that technology and systems used in the company are adequate to properly run the business.

**Financial Aspects of Corporate Governance report (Cadbury report)**

The agency head is responsible for ensuring that the agency has in place procedures for identifying information resources at risk and providing protection for them.  
Senior Management is responsible for, and should support, the implementation and maintenance of information security procedures within the areas under their control.

**National Institute of Standards (NIST) handbook**

According to NIST senior management has ultimate responsibility for the security of an organization's computer systems.

**Governance, Control and Audit for Information and Related Technology (COBIT)**

Control which includes policies, organisational structures, practices and procedures, is management's responsibility. Management, through its **corporate governance**, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance or operation of information systems

**Board Briefing document on IT Governance**

Corporate Governance is to:

- Setting aims
- Providing the leadership to put them into effect
- Supervising the management of the business
- Report to shareholders
- IT resources to be used responsibly

**Information Security Governance: Guidance for Boards of Directors and Executive Management**

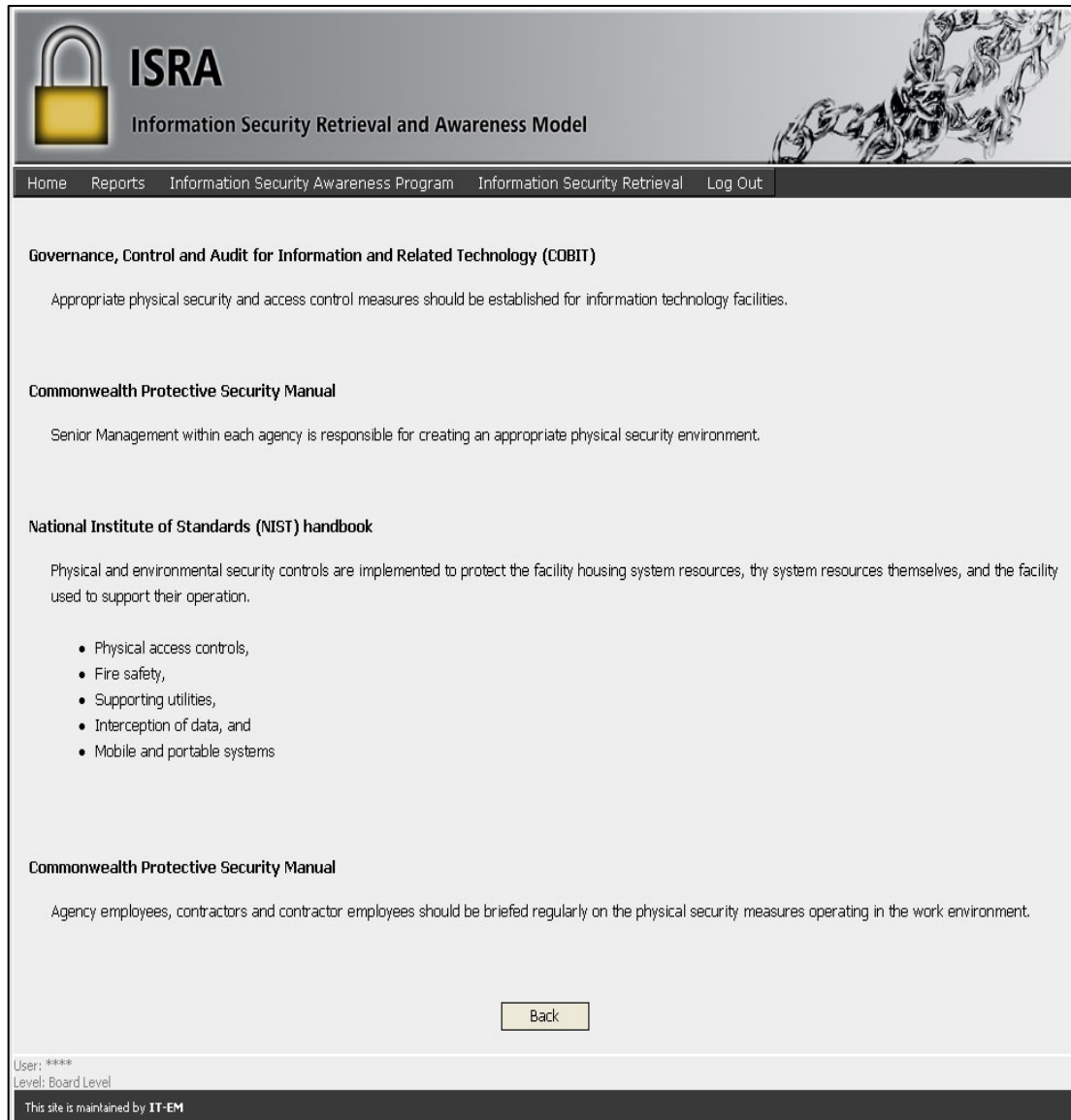
For Information Security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required.

- Understand why information security needs to be governed
- Ensure it fits in the IT Governance framework
- Take Board level action
- Take Management Level action
- Information security policy
- Legal aspects
- Third party testing
- Employee awareness
- Adopt Best Practices

[Back](#)

User: \*\*\*\*  
Level: Board Level  
This site is maintained by IT-EM

**Figure 8.7: Detailed information on corporate governance (including Information Security governance)**

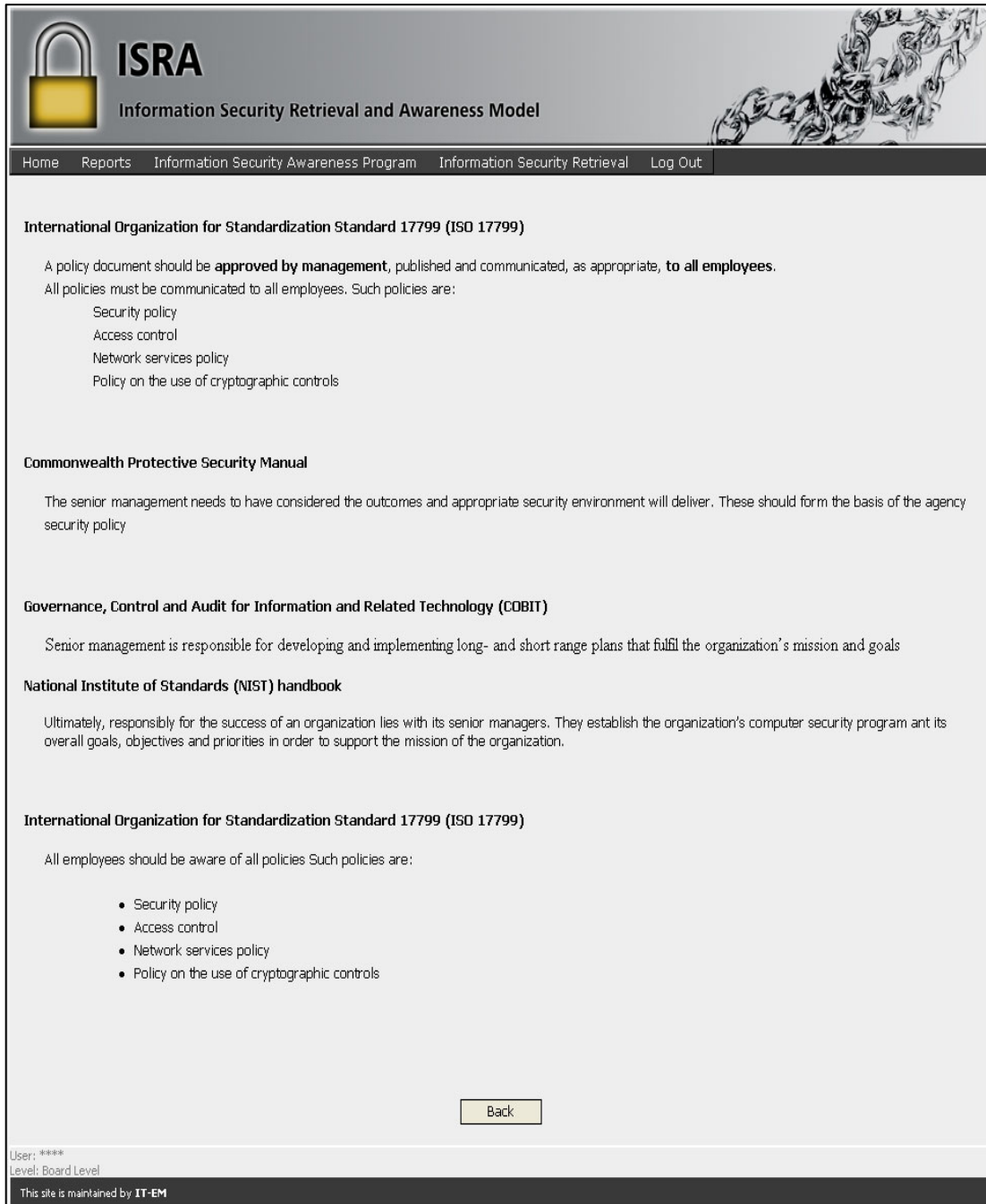


The screenshot displays the ISRA (Information Security Retrieval and Awareness) model implementation. The header features a padlock icon and the text "ISRA Information Security Retrieval and Awareness Model". A navigation menu includes "Home", "Reports", "Information Security Awareness Program", "Information Security Retrieval", and "Log Out". The main content area is divided into sections:

- Governance, Control and Audit for Information and Related Technology (COBIT)**  
Appropriate physical security and access control measures should be established for information technology facilities.
- Commonwealth Protective Security Manual**  
Senior Management within each agency is responsible for creating an appropriate physical security environment.
- National Institute of Standards (NIST) handbook**  
Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facility used to support their operation.
  - Physical access controls,
  - Fire safety,
  - Supporting utilities,
  - Interception of data, and
  - Mobile and portable systems
- Commonwealth Protective Security Manual**  
Agency employees, contractors and contractor employees should be briefed regularly on the physical security measures operating in the work environment.

A "Back" button is located at the bottom center of the content area. The footer shows "User: \*\*\*\*", "Level: Board Level", and "This site is maintained by IT-EM".

*Figure 8.8: Detailed information on physical security*



The screenshot displays the ISRA (Information Security Retrieval and Awareness) model interface. At the top, there is a header with a padlock icon and the text "ISRA Information Security Retrieval and Awareness Model". Below the header is a navigation menu with links for "Home", "Reports", "Information Security Awareness Program", "Information Security Retrieval", and "Log Out". The main content area is divided into several sections, each detailing a different security policy or standard. The first section is titled "International Organization for Standardization Standard 17799 (ISO 17799)" and discusses the approval and communication of policies. The second section is titled "Commonwealth Protective Security Manual" and discusses the role of senior management. The third section is titled "Governance, Control and Audit for Information and Related Technology (COBIT)" and discusses the responsibility of senior management. The fourth section is titled "National Institute of Standards (NIST) handbook" and discusses the responsibility of senior managers. The fifth section is titled "International Organization for Standardization Standard 17799 (ISO 17799)" and discusses the awareness of policies. At the bottom of the main content area, there is a "Back" button. The footer of the page displays the user information: "User: \*\*\*\*", "Level: Board Level", and "This site is maintained by IT-EM".

**ISRA**  
Information Security Retrieval and Awareness Model

Home Reports Information Security Awareness Program Information Security Retrieval Log Out

**International Organization for Standardization Standard 17799 (ISO 17799)**

A policy document should be **approved by management**, published and communicated, as appropriate, **to all employees**.  
All policies must be communicated to all employees. Such policies are:

- Security policy
- Access control
- Network services policy
- Policy on the use of cryptographic controls

**Commonwealth Protective Security Manual**

The senior management needs to have considered the outcomes and appropriate security environment will deliver. These should form the basis of the agency security policy

**Governance, Control and Audit for Information and Related Technology (COBIT)**

Senior management is responsible for developing and implementing long- and short range plans that fulfil the organization's mission and goals

**National Institute of Standards (NIST) handbook**

Ultimately, responsibly for the success of an organization lies with its senior managers. They establish the organization's computer security program ant its overall goals, objectives and priorities in order to support the mission of the organization.

**International Organization for Standardization Standard 17799 (ISO 17799)**

All employees should be aware of all policies Such policies are:

- Security policy
- Access control
- Network services policy
- Policy on the use of cryptographic controls

Back

User: \*\*\*\*  
Level: Board Level  
This site is maintained by IT-EM

**Figure 8.9: Detailed information on security policy**

Having read all the information displayed regarding the non-technical Information Security issues relevant to the Board level, the owner continued by completing one test for each non-technical Information Security issue by clicking the appropriate links. For the purpose of testing the prototype the author constructed the necessary questions and answers for each Information Security awareness test. The number of questions for each test was limited to 16, and selected randomly from the database. The prototype enables

the Information Security Manager to enter the number of questions to be asked for each test.

Figures 8.10 to 8.13 display the screens containing the tests completed by the owner.

Please complete the assessment questions for Computer Ethics

- 1) Ethics is a complex issue.  
 True  
 False
- 2) There is always only one solution to ethical problems.  
 False  
 True
- 3) Ethics is a set of \_\_\_\_\_.  
 rules set by law to determine what is right or wrong  
 principles based on religious rules and regulations  
 principles for justifying what is right or wrong
- 4) There is \_\_\_\_\_ relationship between ethics and computer ethics  
 an indirect  
 no  
 direct
- 5) Ethics is a situational issue.  
 True  
 False
- 6) Ethical principles are pre-identified problems.  
 False  
 True
- 7) All stakeholders should understand what is meant by ethical behaviour.  
 True  
 False
- 8) Ethics can be seen as a set of prescribed rules or a code of behaviour that is to determine between \_\_\_\_\_.  
 all computers  
 all stakeholders

9) Ethical standards are \_\_\_\_principles.

idealistic  
 legal  
 religious

10) Adhering to a Code of Ethics is to do what is right and to \_\_\_\_\_ what is wrong.

report  
 disregard  
 ignore  
 disguise

11) It is unethical to download unauthorised software on your work computer.

False  
 True

12) Ethics should be part of the day-to-day activities of all employees.

True  
 False

13) Copyright is an ethical issue.

False  
 True

14) Ethics is about honesty, fair play, proper compensation and respect for privacy.

False  
 True

15) Ethics is described as \_\_\_\_\_.


legislatures representing all people  
 unwritten principles  
 a formal, written document

16) Ethical conduct may influence your professional status.

True  
 False

User: \*\*\*\*  
Level: Board Level  
This site is maintained by IT-EM

**Figure 8.10: Information Security awareness test for computer ethics**



Home Reports Information Security Awareness Program Information Security Retrieval Log Out

Please complete the assessment questions for Corporate Governance

- 1) Top Management's actions are subject to laws, regulations and shareholders in general meetings.  
 False  
 True
- 2) The Board of Directors is responsible for developing and implementing \_\_\_\_\_ Information Security policies and procedures.  
 no  
 only long-term  
 only short-term  
 long-term and short-term
- 3) Corporate Governance is about compliance with all business practice.  
 False  
 True
- 4) Information Security Governance is \_\_\_\_\_ Risk Governance.  
 more important than  
 less important than  
 just as important as
- 5) Top Management should \_\_\_\_\_ the Information Security Policy.  
 ignore  
 take note of  
 be committed to
- 6) Top Management has the authority to change the Information Security Policy.  
 True  
 False
- 7) Corporate Governance is about effective communication of the company's strategic plans and ethical code, both internally and externally.  
 True  
 False
- 8) Top Management is responsible for ensuring that the organisation has an Information Security Policy.  
 True  
 False

9) The Top Management within each organisation is responsible for creating an Information Security Policy.

False  
 True

10) Information is a \_\_\_\_\_ issue.

technical  
 technical as well as a non-technical  
 non-technical

11) Information Security is a Corporate Governance issue.

False  
 True

12) Top Management could be held accountable by law if information is compromised.

True  
 False

13) A virus is a program that \_\_\_\_\_.

overtly does one thing while covertly doing another  
 spread its infection from one computer to another  
 has secret entry points  
 makes information accessible to unauthorised people

14) Top Management \_\_\_\_\_ for all information.

is not accountable  
 is accountable

15) Users have the authority to change the Information Security Policy.

True  
 False


16) An Information Security Policy is a set of documentation that contains \_\_\_\_\_.

Information Security ideas  
 Information Security rules and regulations  
 Information Security suggestions

User: \*\*\*\*  
Level: Board Level  
This site is maintained by IT-EM

**Figure 8.11: Information Security awareness test for corporate governance**





# ISRA

Information Security Retrieval and Awareness Model

[Home](#) [Reports](#) [Information Security Awareness Program](#) [Information Security Retrieval](#) [Log Out](#)

Please complete the assessment questions for Physical Security

- 1) It is important to ensure that no unauthorised people are able to access information.  
 False  
 True
- 2) Personal computers, laptops and personal digital assistants could pose a physical risk.  
 False  
 True
- 3) Back-up procedures should be included in the Physical Security Policy.  
 False  
 True
- 4) Physical Security is only man made threats  
 True  
 False
- 5) Appropriate physical security and access control measures should be established for information technology.  
 True  
 False
- 6) Physical Security is a \_\_\_\_\_ issue.  
 technical and non-technical  
 technical  
 non-technical
- 7) Fire safety should be part of the Physical Security Policy.  
 False  
 True
- 8) Employees, contractors and contractor employees should be briefed regularly on the physical security measures operating in their work environment.  
 True  
 False

9) Physical Security is about protecting the computer system from \_\_\_\_\_.

people outside the organisation  
 all people  
 people inside the organisation

10) Users should \_\_\_\_\_ the Physical Security Policy.

be committed to  
 ignore  
 take note of

11) Physical security describes protection needed outside the computer system.

False  
 True

12) Physical Security is not part of the overall security policy.

True  
 False

13) It is advisable to write down your password on your desk pad.

False  
 True

14) Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facility used to support their operation.

False  
 True

15) Physical Security controls the \_\_\_\_\_ of all stakeholders.

entry and exit  
 entry  
 exit

16) Physical Security is about preventing access to information.

False  
 True

User: \*\*\*\*  
Level: Board Level  
This site is maintained by IT-EM

**Figure 8.12: Information Security awareness test for physical security**



---

[Home](#)   [Reports](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Security Policy

1) Authorisation is \_\_\_\_\_.

- ensuring that information is not disclosed to any unauthorised party
- ensuring that no action that was taken and that affects Information Security can be denied at a later stage
- determining whether or not the authenticated party has the right to access the information
- ensuring that information is still in its original form and that no tampering or alteration has taken place

2) Users have the authority to change the Information Security Policy.

- True
- False

3) Integrity involves making sure \_\_\_\_\_.

- that no action that was taken and that affects Information Security can be denied at a later stage
- that information is not disclosed to any unauthorised party
- whether or not the authenticated party has the right to access the information
- that information is still in its original form and that no tampering or alteration has taken place

4) Compliance Monitoring should be conducted \_\_\_\_\_.

- whenever you remember
- regularly
- as soon as an Information Security incident occurs
- once a year

5) Confidentiality is \_\_\_\_\_.

- ensuring that information is not disclosed to any unauthorised party
- ensuring that no action that was taken and that affects Information Security can be denied at a later stage
- ensuring that information is still in its original form and that no tampering or alteration has taken place

6) The Security Policy should contain \_\_\_\_\_ on how to implement Information Security.

- procedures
- guidelines
- processes, procedures and guidelines
- processes

7) Passwords should be chosen based on your own birthday or surname, or on those of a family member.

- True
- False

8) Non-repudiation is \_\_\_\_\_.

- ensuring that information is not disclosed to any unauthorised party
- ensuring that no action that was taken and that affects Information Security can be denied at a later stage
- determining whether or not the authenticated party has the right to access the information
- ensuring that information is still in its original form and that no tampering or alteration has taken place

Chapter 8

140

9) A password should be \_\_\_\_\_.

complex  
 easy  
 short  
 only characters

10) A trapdoor is a \_\_\_\_\_.

code that makes information accessible to unauthorised  
 program that overly does one thing while covertly doing another  
 program that has secret entry points

11) The Information Security Policy must be distributed to \_\_\_\_\_.

only new stakeholders  
 all stakeholders

12) Users should \_\_\_\_\_ the Information Security Policy.

take note of  
 be committed to  
 ignore

13) An information policy should incorporate new technologies.

False  
 True

14) The Information Security Policy serves as the basis for establishing employees' accountability.

False  
 True

15) An information leak is a \_\_\_\_\_.

program that overly does one thing while covertly doing another  
 code that makes information accessible to unauthorised people  
 program that has secret entry points

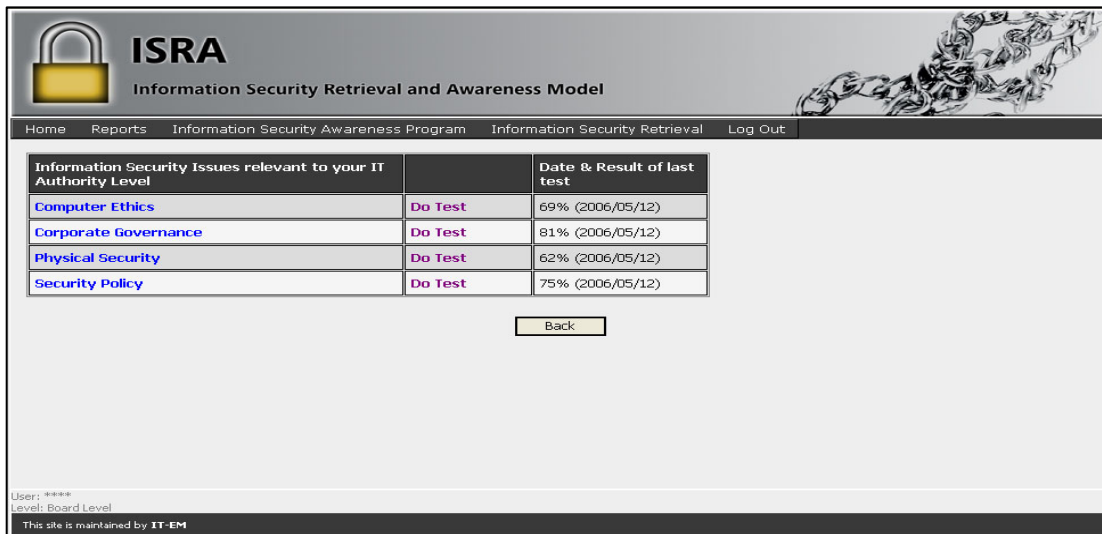
16) The Information Security Policy should consist of subpolicies.

True  
 False

User: \*\*\*\*  
Level: Board Level

**Figure 8.13: Information Security awareness test for security policy**

After each test had been completed, the initial screen (depicted in Figure 8.5) was updated to reflect the results (see Figure 8.14).



The screenshot shows the ISRA web application interface. At the top left is a padlock icon and the text 'ISRA Information Security Retrieval and Awareness Model'. A navigation bar contains links for Home, Reports, Information Security Awareness Program, Information Security Retrieval, and Log Out. The main content area features a table with the following data:

Information Security Issues relevant to your IT Authority Level		Date & Result of last test
<a href="#">Computer Ethics</a>	Do Test	69% (2006/05/12)
<a href="#">Corporate Governance</a>	Do Test	81% (2006/05/12)
<a href="#">Physical Security</a>	Do Test	62% (2006/05/12)
<a href="#">Security Policy</a>	Do Test	75% (2006/05/12)

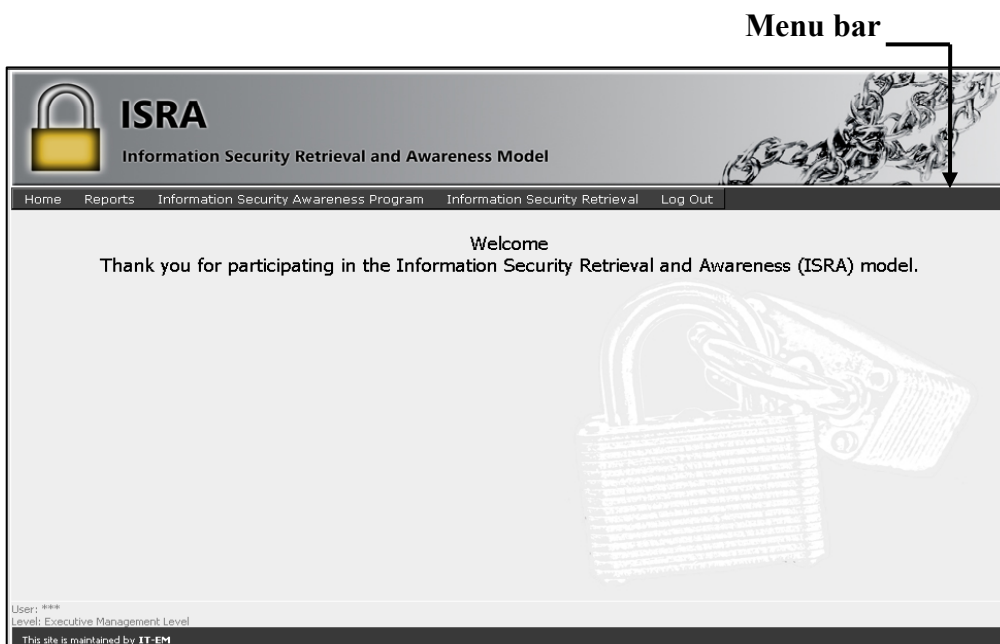
Below the table is a 'Back' button. At the bottom left, the user information is displayed: 'User: \*\*\*\*', 'Level: Board Level', and 'This site is maintained by IT-EM'.

*Figure 8.14: Results for tests taken*

The 'Date & Result of last test' column in Figure 8.14 displays the result for each test, as well as the date on which each test was completed.

### 8.4.1.2 Executive Management level

The Executive Management level of Bekker & du Toit Optometrists consists of one stakeholder, namely the partner. Figure 8.15 depicts the different menu options on the menu bar that are available to the partner after having logged in successfully.



*Figure 8.15: Home screen for Executive Management level*

The first option selected by the partner was the Information Security Awareness Program option on the menu bar. The screen that was displayed as a result is depicted in Figure 8.16.

Information Security Issues relevant to your IT Authority Level	Do Test	Date & Result of last test
<a href="#">Computer Ethics</a>	<a href="#">Do Test</a>	No Result
<a href="#">Corporate Governance</a>	<a href="#">Do Test</a>	No Result
<a href="#">Physical Security</a>	<a href="#">Do Test</a>	No Result
<a href="#">Security Policy</a>	<a href="#">Do Test</a>	No Result

Back

User: \*\*\*  
Level: Executive Management Level  
This site is maintained by IT-EM

**Figure 8.16: Information Security Awareness Program screen**

This screen lists all the non-technical Information Security issues relevant to the Executive Management level, with links so as to access information related to a specific Information Security issue (with a view to preparing for a test). Links are also provided to complete an Information Security awareness test for each issue. In addition, the screen displays the date and the result (0%-100%) of the last competed test. So far no tests have been completed by the partner.

The partner first viewed information on each non-technical Information Security issue listed by clicking on the appropriate link. Figures 8.17 to 8.20 depict the screens that were displayed when the owner clicked on the Computer Ethics, Corporate Governance, Physical Security and Security Policy links respectively.



The screenshot displays the ISRA (Information Security Retrieval and Awareness Model) website. The header features a logo with a padlock and the text 'ISRA Information Security Retrieval and Awareness Model'. A navigation menu includes 'Home', 'Reports', 'Information Security Awareness Program', 'Information Security Retrieval', and 'Log Out'. The main content area is titled 'Governance, Control and Audit for Information and Related Technology (COBIT)' and contains three sections: 'Governance, Control and Audit for Information and Related Technology (COBIT)', 'Commonwealth Protective Security Manual', and 'The KING report'. Each section provides detailed text on organizational frameworks, ethical values, and security procedures. A 'Back' button is located at the bottom of the content area. The footer includes user information: 'User: \*\*\*', 'Level: Executive Management Level', and 'This site is maintained by IT-EM'.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Reports Information Security Awareness Program Information Security Retrieval Log Out

**Governance, Control and Audit for Information and Related Technology (COBIT)**

Management should create a framework and an awareness programme fostering a positive control environment throughout the entire organisation by addressing aspects such as: integrity, **ethical values** and competence of the people; management philosophy and operating style; and accountability, attention and direction provided by the board of directors.

Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the policies and procedures are being followed. Compliance procedures for **ethical**, security and internal control standards should be set by top management and promoted by example.

All personnel should be trained and educated in system security principles. Senior management should provide an education and training programme that includes: ethical conduct of the information services function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.

**Commonwealth Protective Security Manual**

The agency head is responsible for ensuring that the agency has in place procedures for identifying information resources at risk and providing protection for them.

Senior Management is responsible for, and should support, the implementation and maintenance of information security procedures within the areas under their control.

**The KING report**

Establish the values of the enterprise in support of its vision and mission

Establish principles and standards of ethical business practice for the enterprise in support of such values

Ensure communication of established principles and standards to affected stakeholders in codified form

Assume responsibility and accountability to stakeholders for compliance with such principles and standards.

Effective communication of its strategic plans and ethical code both internally and externally.

**Governance, Control and Audit for Information and Related Technology (COBIT)**

Management should create a framework and an awareness programme fostering a positive control environment throughout the entire organisation by addressing aspects such as: integrity, **ethical values** and competence of the people; management philosophy and operating style; and accountability, attention and direction provided by the board of directors.

Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the policies and procedures are being followed. Compliance procedures for **ethical**, security and internal control standards should be set by top management and promoted by example.

All personnel should be trained and educated in system security principles. Senior management should provide an education and training programme that includes: ethical conduct of the information services function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.

[Back](#)

User: \*\*\*  
Level: Executive Management Level  
This site is maintained by IT-EM

*Figure 8.17: Detailed information on computer ethics*



The screenshot displays the ISRA (Information Security Retrieval and Awareness Model) website. The header features a padlock icon and the text 'ISRA Information Security Retrieval and Awareness Model'. A navigation bar includes links for Home, Reports, Information Security Awareness Program, Information Security Retrieval, and Log Out. The main content area is titled 'Governance, Control and Audit for Information and Related Technology (COBIT)' and contains several sections:

- Governance, Control and Audit for Information and Related Technology (COBIT)**: A paragraph explaining that control, including policies, structures, practices, and procedures, is management's responsibility. Management, through its corporate governance, must ensure due diligence is exercised by all individuals involved in the management, use, design, development, maintenance, or operation of information systems.
- The KING report**: A list of three points: effective communication of strategic plans and ethical code; compliance with all business practices; and ensuring procedures and practices protect the company's assets and that technology and systems are adequate for proper business operation.
- Financial Aspects of Corporate Governance report (Cadbury report)**: A paragraph stating that the agency head is responsible for ensuring in-place procedures for identifying information resources at risk and providing protection, and that senior management should support the implementation and maintenance of information security procedures.
- Board Briefing document on IT Governance**: A list of five points: setting aims; providing leadership to put them into effect; supervising the management of the business; reporting to shareholders; and using IT resources responsibly.
- Information Security Governance: Guidance for Boards of Directors and Executive Management**: A paragraph stating that greater involvement of boards, executive management, and business process owners is required, followed by a list of seven points: understanding why information security needs to be governed; ensuring it fits in the IT Governance framework; taking Board and Management Level action; information security policy; legal aspects; third party testing; employee awareness; and adopting best practices.
- National Institute of Standards (NIST) handbook**: A paragraph stating that according to NIST, senior management has ultimate responsibility for the security of an organization's computer systems.

A 'Back' button is located at the bottom center of the content area. The footer includes the text: 'User: \*\*\*', 'Level: Executive Management Level', and 'This site is maintained by IT-EM'.

**Figure 8.18: Detailed information on corporate governance (including Information Security governance)**





The screenshot displays the ISRA (Information Security Retrieval and Awareness) model implementation website. The header features a yellow padlock icon and the text "ISRA Information Security Retrieval and Awareness Model". A navigation menu includes "Home", "Reports", "Information Security Awareness Program", "Information Security Retrieval", and "Log Out". The main content area is titled "Governance, Control and Audit for Information and Related Technology (COBIT)" and contains the following text: "Appropriate physical security and access control measures should be established for information technology facilities." Below this, the "National Institute of Standards (NIST) handbook" section states: "Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facility used to support their operation." A bulleted list follows: "Physical access controls, Fire safety, Supporting utilities, Interception of data, and Mobile and portable systems". The "Commonwealth Protective Security Manual" section is repeated twice, with the first instance stating: "Senior Management within each agency is responsible for creating an appropriate physical security environment." and the second instance stating: "Agency employees, contractors and contractor employees should be briefed regularly on the physical security measures operating in the work environment." A "Back" button is located at the bottom center. The footer shows "User: \*\*\*", "Level: Executive Management Level", and "This site is maintained by IT-EM".

**ISRA**  
Information Security Retrieval and Awareness Model

Home Reports Information Security Awareness Program Information Security Retrieval Log Out

**Governance, Control and Audit for Information and Related Technology (COBIT)**

Appropriate physical security and access control measures should be established for information technology facilities.

**National Institute of Standards (NIST) handbook**

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facility used to support their operation.

- Physical access controls,
- Fire safety,
- Supporting utilities,
- Interception of data, and
- Mobile and portable systems

**Commonwealth Protective Security Manual**

Senior Management within each agency is responsible for creating an appropriate physical security environment.

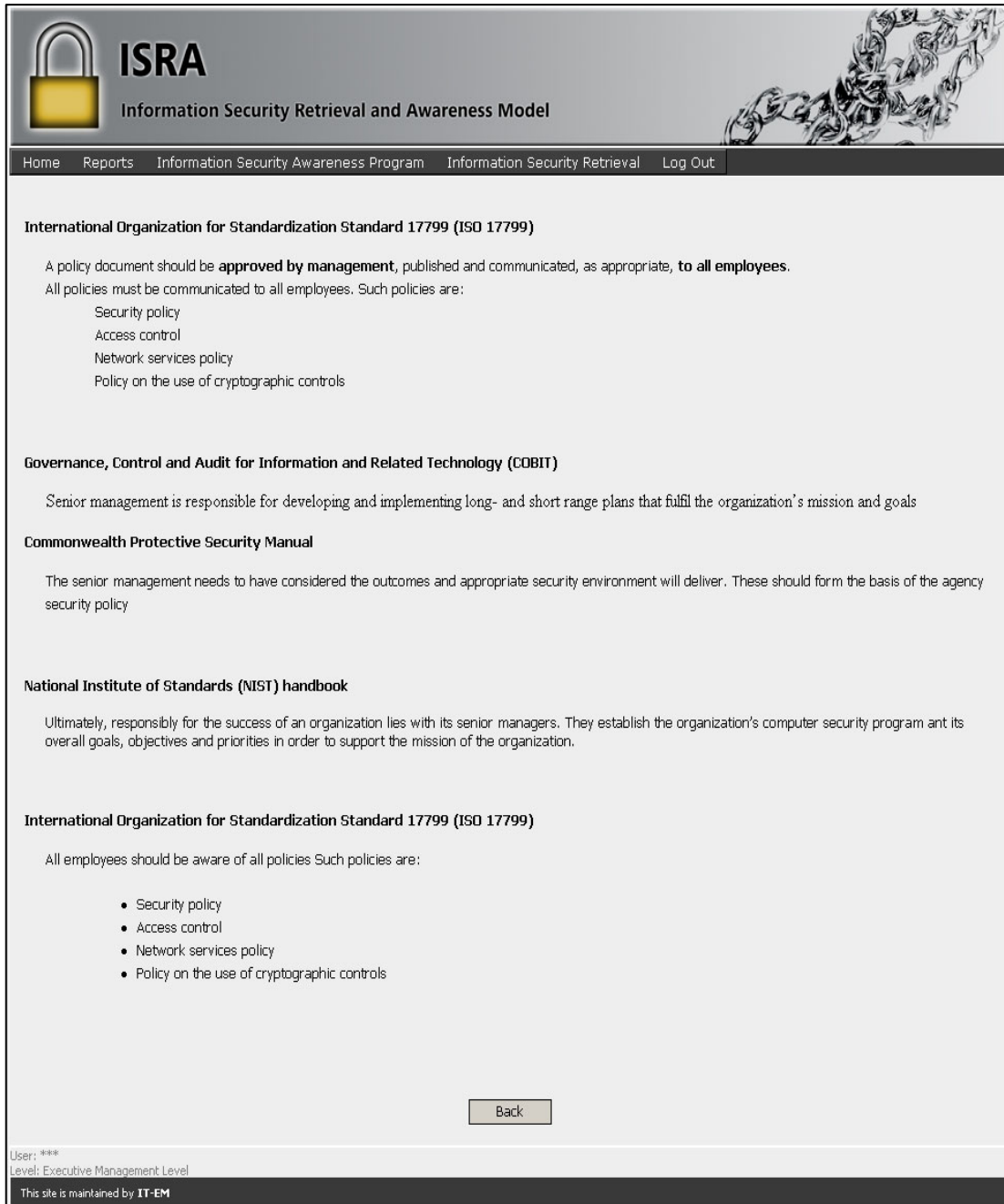
**Commonwealth Protective Security Manual**

Agency employees, contractors and contractor employees should be briefed regularly on the physical security measures operating in the work environment.

[Back](#)

User: \*\*\*  
Level: Executive Management Level  
This site is maintained by IT-EM

*Figure 8.19: Detailed information on physical security*



**ISRA**  
Information Security Retrieval and Awareness Model

Home Reports Information Security Awareness Program Information Security Retrieval Log Out

**International Organization for Standardization Standard 17799 (ISO 17799)**

A policy document should be **approved by management**, published and communicated, as appropriate, **to all employees**.  
All policies must be communicated to all employees. Such policies are:

- Security policy
- Access control
- Network services policy
- Policy on the use of cryptographic controls

**Governance, Control and Audit for Information and Related Technology (COBIT)**

Senior management is responsible for developing and implementing long- and short range plans that fulfil the organization's mission and goals

**Commonwealth Protective Security Manual**

The senior management needs to have considered the outcomes and appropriate security environment will deliver. These should form the basis of the agency security policy

**National Institute of Standards (NIST) handbook**

Ultimately, responsibility for the success of an organization lies with its senior managers. They establish the organization's computer security program and its overall goals, objectives and priorities in order to support the mission of the organization.

**International Organization for Standardization Standard 17799 (ISO 17799)**

All employees should be aware of all policies Such policies are:


- Security policy
- Access control
- Network services policy
- Policy on the use of cryptographic controls

Back

User: \*\*\*  
Level: Executive Management Level  
This site is maintained by IT-EM


**Figure 8.20: Detailed information on security policy**

Having read all the information that was displayed regarding the non-technical Information Security issues relevant to the Executive Management level, the partner continued by completing one test for each non-technical Information Security issue by clicking the appropriate links. Figures 8.21 to 8.24 display the screens containing the tests completed by the partner.



## ISRA

Information Security Retrieval and Awareness Model



---

[Home](#)   [Reports](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Computer Ethics

- Ethics is a set of \_\_\_\_\_.
  - rules set by law to determine what is right or wrong
  - principles based on religious rules and regulations
  - principles for justifying what is right or wrong
- It is unethical to download unauthorised software on your work computer.
  - False
  - True
- All stakeholders should understand what is meant by ethical behaviour.
  - True
  - False
- Copyright is an ethical issue.
  - False
  - True
- Ethics is about honesty, fair play, proper compensation and respect for privacy.
  - False
  - True
- Ethics is a complex issue.
  - True
  - False
- Adhering to a Code of Ethics is to do what is right and to \_\_\_\_\_ what is wrong.
  - report
  - disregard
  - ignore
  - disguise
- Ethical principles are pre-identified problems.
  - False
  - True

Chapter 8

148

9) There is \_\_\_\_\_ relationship between ethics and computer ethics

an indirect  
 no  
 direct

10) Ethical standards are \_\_\_\_\_ principles.

idealistic  
 legal  
 religious

11) Ethics should be part of the day-to-day activities of all employees.

True  
 False

12) There is always only one solution to ethical problems.

False  
 True

13) Ethics can be seen as a set of prescribed rules or a code of behaviour that is to determine between \_\_\_\_\_.

all computers  
 all stakeholders

14) Ethics is described as \_\_\_\_\_.

legislatures representing all people  
 unwritten principles  
 a formal, written document

15) Ethics is a situational issue.


True  
 False

16) Ethical conduct may influence your professional status.

True  
 False


User: \*\*\*  
Level: Executive Management Level  
This site is maintained by IT-EM

**Figure 8.21: Information Security awareness test for computer ethics**



## ISRA

Information Security Retrieval and Awareness Model



---

[Home](#)   [Reports](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Corporate Governance

- 1) Top Management should \_\_\_\_\_ the Information Security Policy.  
 ignore  
 take note of  
 be committed to
- 2) Top Management is responsible for distributing the Information Security Policy to all stakeholders.  
 False  
 True
- 3) Top Management \_\_\_\_\_ for all information.  
 is not accountable  
 is accountable
- 4) Corporate Governance is about effective communication of the company's strategic plans and ethical code, both internally and externally.  
 True  
 False
- 5) Top Management could be held accountable by law if information is compromised.  
 True  
 False
- 6) Corporate Governance is about compliance with all business practice.  
 False  
 True
- 7) Information Security Governance is \_\_\_\_\_ Risk Governance.  
 more important than  
 less important than  
 just as important as
- 8) Information Security is a Corporate Governance Issue.  
 False  
 True

9) The Board of Directors is responsible for developing and implementing \_\_\_\_\_ Information Security policies and procedures.

no  
 only long-term  
 only short-term  
 long-term and short-term

10) Users have the authority to change the Information Security Policy.

True  
 False

11) An Information Security Policy is a set of documentation that contains \_\_\_\_\_.

Information Security Ideas  
 Information Security rules and regulations  
 Information Security suggestions

12) Top Management's actions are subject to laws, regulations and shareholders in general meetings.

False  
 True

13) A virus is a program that \_\_\_\_\_.

overtly does one thing while covertly doing another  
 spread its infection from one computer to another  
 has secret entry points  
 makes information accessible to unauthorised people

14) Information is a \_\_\_\_\_ issue.

technical  
 technical as well as a non-technical  
 non-technical

15) The Top Management within each organisation is responsible for creating an Information Security Policy.


False  
 True

16) Top Management has the authority to change the Information Security Policy.

True  
 False


User: \*\*\*  
Level: Executive Management Level  
This site is maintained by IT-EM

**Figure 8.22: Information Security awareness test for corporate governance**



## ISRA

Information Security Retrieval and Awareness Model



---

[Home](#)   [Reports](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Physical Security

- Physical Security is only man made threats.  
 True  
 False
- Physical Security is a \_\_\_\_\_ issue.  
 technical and non-technical  
 technical  
 non-technical
- Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facility used to support their operation.  
 False  
 True
- It is important to ensure that no unauthorised people are able to access information.  
 False  
 True
- Physical security describes protection needed outside the computer system.  
 False  
 True
- Physical Security is about preventing access to information.  
 False  
 True
- Appropriate physical security and access control measures should be established for information technology.  
 True  
 False
- Physical Security is about protecting the computer system from \_\_\_\_\_.  
 people outside the organisation  
 all people  
 people inside the organisation

9) Personal computers, laptops and personal digital assistants could pose a physical risk.

False  
 True

10) Physical Security controls the \_\_\_\_\_ of all stakeholders.

entry and exit  
 entry  
 exit

11) Physical Security is not part of the overall security policy.

True  
 False

12) Users should \_\_\_\_\_ the Physical Security Policy.

be committed to  
 ignore  
 take note of

13) Fire safety should be part of the Physical Security Policy.

False  
 True

14) Back-up procedures should be included in the Physical Security Policy.

False  
 True

15) It is advisable to write down your password on your desk pad.

False  
 True

16) Employees, contractors and contractor employees should be briefed regularly on the physical security measures operating in their work environment.

True  
 False

User: \*\*\*  
Level: Executive Management Level  
This site is maintained by IT-EM

**Figure 8.23: Information Security awareness test for physical security**





Home   Reports   Information Security Awareness Program   Information Security Retrieval   Log Out

Please complete the assessment questions for Security Policy

1) The Information Security Policy must be distributed to \_\_\_\_\_.

only new stakeholders  
 all stakeholders

2) Users have the authority to change the Information Security Policy.

True  
 False

3) Users should \_\_\_\_\_ the Information Security Policy.

take note of  
 be committed to  
 ignore

4) Authorisation is \_\_\_\_\_.

ensuring that information is not disclosed to any unauthorised party  
 ensuring that no action that was taken and that affects Information Security can be denied at a later stage  
 determining whether or not the authenticated party has the right to access the information  
 ensuring that information is still in its original form and that no tampering or alteration has taken place

5) An information leak is a \_\_\_\_\_.

program that overly does one thing while covertly doing another  
 code that makes information accessible to unauthorised people  
 program that has secret entry points

6) Compliance Monitoring should be conducted \_\_\_\_\_.

whenever you remember  
 regularly  
 as soon as an Information Security incident occurs  
 once a year

7) A password should be \_\_\_\_\_.

complex  
 easy  
 short  
 only characters

8) Integrity involves making sure \_\_\_\_\_.

that no action that was taken and that affects Information Security can be denied at a later stage  
 that information is not disclosed to any unauthorised party  
 whether or not the authenticated party has the right to access the information  
 that information is still in its original form and that no tampering or alteration has taken place

9) The Security Policy should contain \_\_\_\_\_ on how to implement Information Security.

procedures  
 guidelines  
 processes, procedures and guidelines  
 processes

10) Passwords should be chosen based on your own birthday or surname, or on those of a family member.

True  
 False

11) Non-repudiation is \_\_\_\_\_.

ensuring that information is not disclosed to any unauthorised party  
 ensuring that no action that was taken and that affects Information Security can be denied at a later stage  
 determining whether or not the authenticated party has the right to access the information  
 ensuring that information is still in its original form and that no tampering or alteration has taken place

12) An information policy should incorporate new technologies.

False  
 True

13) The Information Security Policy should consist of subpolicies.

True  
 False

14) Confidentiality is \_\_\_\_\_.

ensuring that information is not disclosed to any unauthorised party  
 ensuring that no action that was taken and that affects Information Security can be denied at a later stage  
 ensuring that information is still in its original form and that no tampering or alteration has taken place

15) A trapdoor is a \_\_\_\_\_.

code that makes information accessible to unauthorised  
 program that overly does one thing while covertly doing another  
 program that has secret entry points

16) Top Management has the authority to change the Information Security Policy.

False  
 True

User: \*\*\*  
Level: Executive Management Level  
This site is maintained by IT-EM

**Figure 8.24: Information Security awareness test for security policy**

After each test was completed, the initial screen (depicted in Figure 8.16) was updated to reflect the result (see Figure 8.25).

The screenshot shows the ISRA web application interface. At the top left is the ISRA logo (a padlock) and the text 'ISRA Information Security Retrieval and Awareness Model'. A navigation bar contains links for 'Home', 'Reports', 'Information Security Awareness Program', 'Information Security Retrieval', and 'Log Out'. The main content area features a table with the following data:

Information Security Issues relevant to your IT Authority Level		Date & Result of last test
Computer Ethics	Do Test	50% (2006/05/12)
Corporate Governance	Do Test	88% (2006/05/12)
Physical Security	Do Test	81% (2006/05/12)
Security Policy	Do Test	62% (2006/05/12)

Below the table is a 'Back' button. At the bottom left, it shows 'User: \*\*\*' and 'Level: Executive Management Level'. A footer note states 'This site is maintained by IT-EM'.

Figure 8.25: Results for test taken

The ‘Date & Result of last test’ column in Figure 8.25 displays the result for each test, as well as the date on which each test was completed.

### 8.4.1.3 User level

The User level of Bekker & du Toit Optometrist consists of two stakeholders – the secretary and an accountant. Figure 8.26 depicts the different menu options on the menu bar that are available to the users after they have logged in successfully.

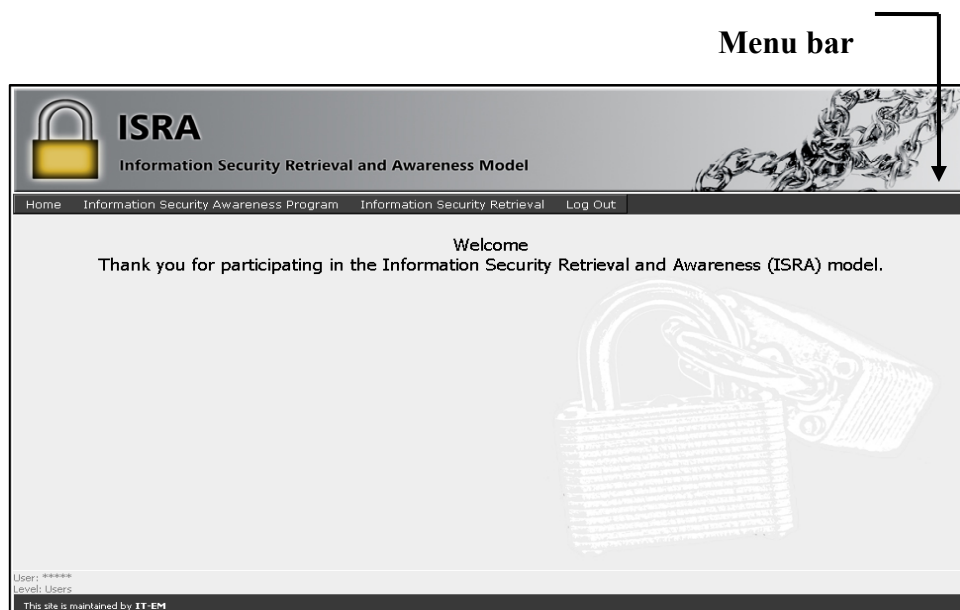
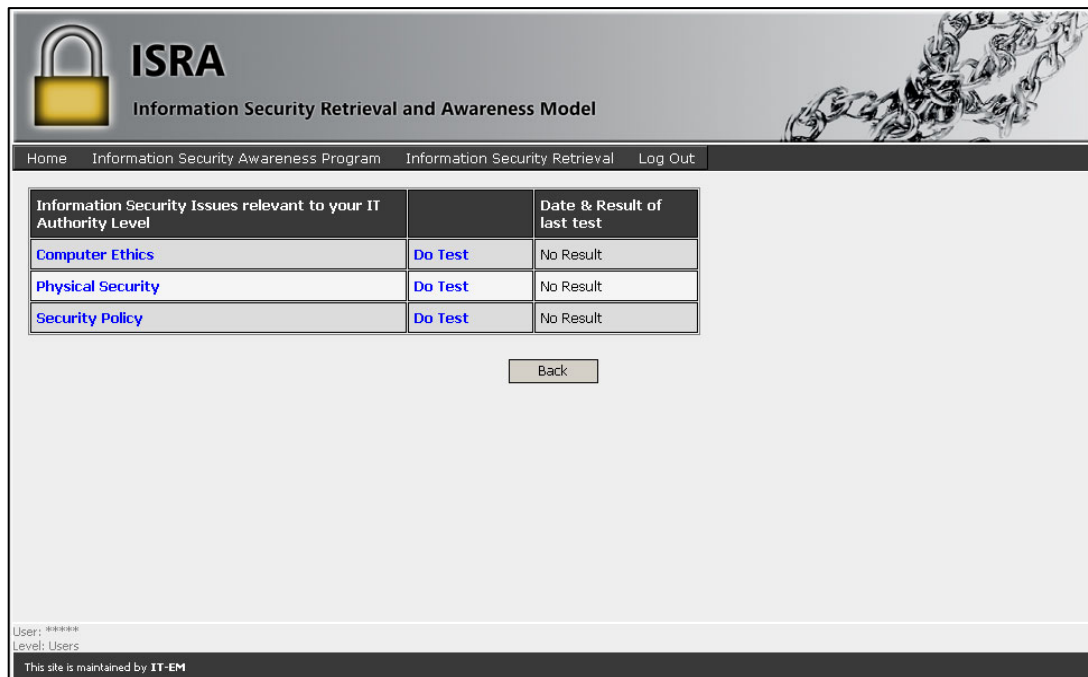


Figure 8.26: Home screen for User level

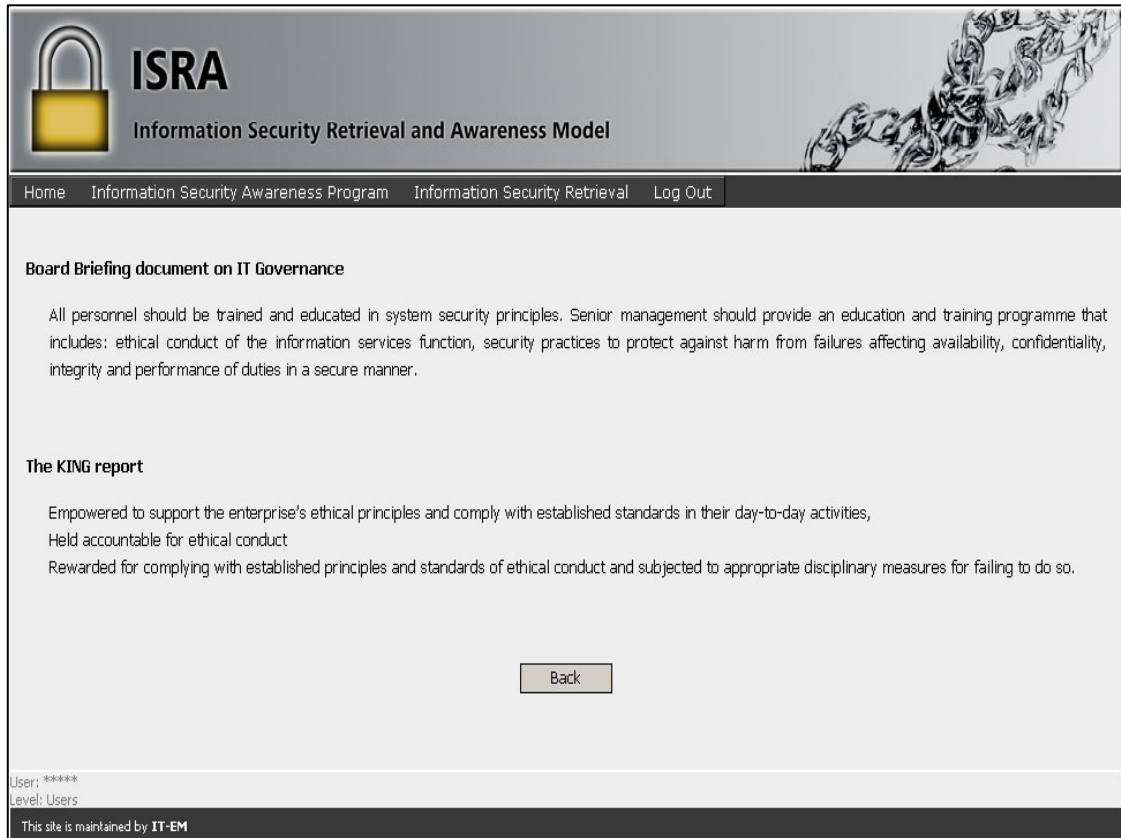
The first option selected by the secretary was the Information Security Awareness Program option on the menu bar and the screen that was subsequently displayed is depicted in Figure 8.27.



**Figure 8.27: Information Security Awareness Program screen**

The screen lists all the non-technical Information Security issues relevant to the User level, with links to access information related to a specific Information Security issue (i.e. with a view to preparing for a test). In addition, links to complete an Information Security awareness test for each issue are provided. The screen also displays the date and the result (0%-100%) of the last completed test – so far no tests have been completed by the secretary.

The secretary first viewed information on each non-technical Information Security issue that was listed by clicking on the appropriate link. Figures 8.28 to 8.30 depict the screens that were displayed when the secretary clicked on the Computer Ethics, Physical Security and Security Policy links respectively.



The screenshot shows the ISRA website interface. At the top left is a yellow padlock icon next to the text "ISRA Information Security Retrieval and Awareness Model". A navigation bar contains links for "Home", "Information Security Awareness Program", "Information Security Retrieval", and "Log Out". The main content area features a section titled "Board Briefing document on IT Governance" with a paragraph of text. Below it is a section titled "The KING report" with three bullet points. A "Back" button is centered at the bottom of the content area. The footer includes "User: \*\*\*\*\*", "Level: Users", and "This site is maintained by IT-EM".

**ISRA**  
Information Security Retrieval and Awareness Model

Home Information Security Awareness Program Information Security Retrieval Log Out

**Board Briefing document on IT Governance**

All personnel should be trained and educated in system security principles. Senior management should provide an education and training programme that includes: ethical conduct of the information services function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.

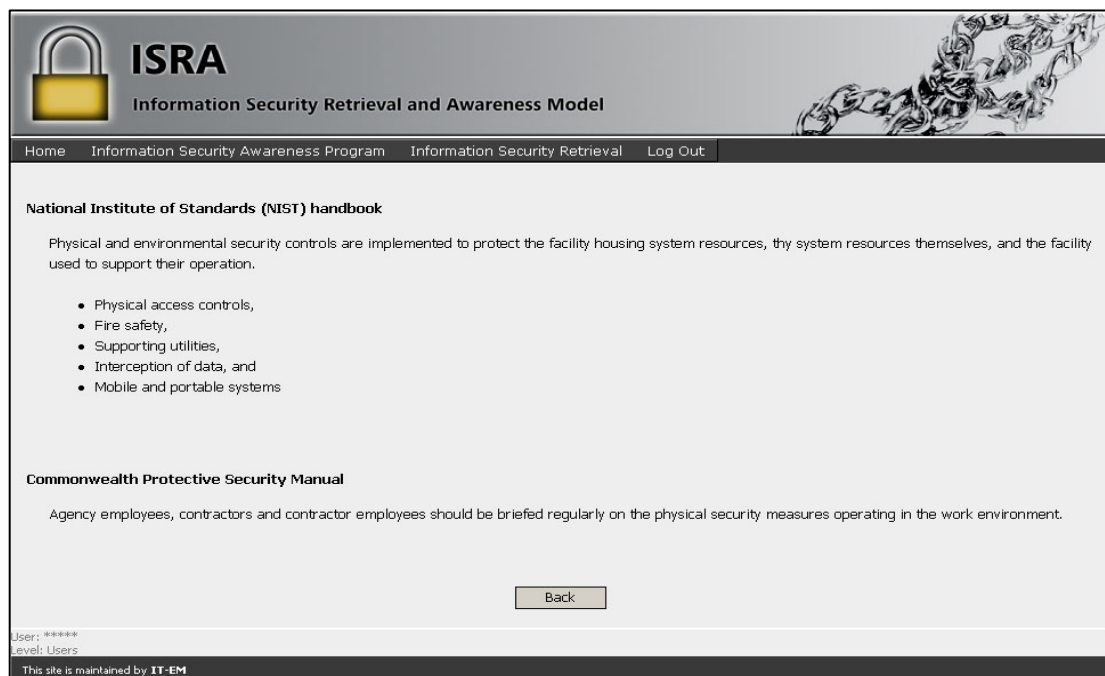
**The KING report**

- Empowered to support the enterprise's ethical principles and comply with established standards in their day-to-day activities,
- Held accountable for ethical conduct
- Rewarded for complying with established principles and standards of ethical conduct and subjected to appropriate disciplinary measures for failing to do so.

Back

User: \*\*\*\*\*  
Level: Users  
This site is maintained by IT-EM

*Figure 8.28: Detailed information on computer ethics*



The screenshot shows the ISRA website interface. At the top left is a yellow padlock icon next to the text "ISRA Information Security Retrieval and Awareness Model". A navigation bar contains links for "Home", "Information Security Awareness Program", "Information Security Retrieval", and "Log Out". The main content area features a section titled "National Institute of Standards (NIST) handbook" with a paragraph of text and a bulleted list. Below it is a section titled "Commonwealth Protective Security Manual" with a paragraph of text. A "Back" button is centered at the bottom of the content area. The footer includes "User: \*\*\*\*\*", "Level: Users", and "This site is maintained by IT-EM".

**ISRA**  
Information Security Retrieval and Awareness Model

Home Information Security Awareness Program Information Security Retrieval Log Out

**National Institute of Standards (NIST) handbook**

Physical and environmental security controls are implemented to protect the facility housing system resources, thy system resources themselves, and the facility used to support their operation.

- Physical access controls,
- Fire safety,
- Supporting utilities,
- Interception of data, and
- Mobile and portable systems

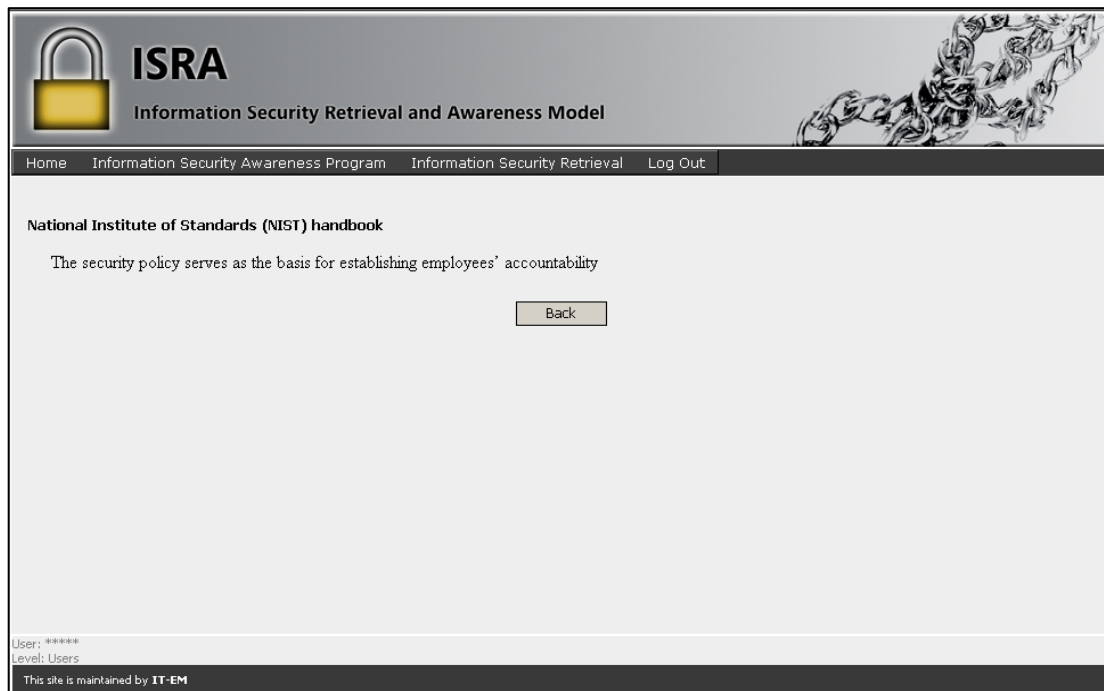
**Commonwealth Protective Security Manual**

Agency employees, contractors and contractor employees should be briefed regularly on the physical security measures operating in the work environment.

Back

User: \*\*\*\*\*  
Level: Users  
This site is maintained by IT-EM


*Figure 8.29: Detailed information on physical security*



*Figure 8.30: Detailed information on security policy*


The accountant also first selected the Information Security Awareness Program option on the menu bar, and followed the exact same steps as the secretary to view information on each Information Security issue.

Having read all the information displayed about the non-technical Information Security issues that are relevant to the User level, the secretary and the accountant continued to complete one test for each non-technical Information Security issue by clicking on the appropriate links. The screens containing the tests that were completed by the secretary are displayed in Figures 8.31 to 8.33.



## ISRA

Information Security Retrieval and Awareness Model



---

[Home](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Computer Ethics

- Ethics is a situational issue.  
 True  
 False
- Copyright is an ethical issue.  
 False  
 True
- There is \_\_\_\_\_ relationship between ethics and computer ethics  
 an indirect  
 no  
 direct
- Ethics can be seen as a set of prescribed rules or a code of behaviour that is to determine between \_\_\_\_\_.  
 all computers  
 all stakeholders
- Ethics is a set of \_\_\_\_\_.  
 rules set by law to determine what is right or wrong  
 principles based on religious rules and regulations  
 principles for justifying what is right or wrong
- Ethics is about honesty, fair play, proper compensation and respect for privacy.  
 False  
 True
- Ethical standards are \_\_\_\_principles.  
 idealistic  
 legal  
 religious
- Ethics is a complex issue.  
 True  
 False

9) All stakeholders should understand what is meant by ethical behaviour.

True  
 False

10) There is always only one solution to ethical problems.

False  
 True

11) Adhering to a Code of Ethics is to do what is right and to \_\_\_\_\_ what is wrong.

report  
 disregard  
 ignore  
 disguise

12) Ethics should be part of the day-to-day activities of all employees.

True  
 False

13) It is unethical to download unauthorised software on your work computer.

False  
 True

14) Ethics is described as \_\_\_\_\_.

legislatures representing all people  
 unwritten principles  
 a formal, written document

15) Ethical principles are pre-identified problems.

False  
 True

16) Ethical conduct may influence your professional status.

True  
 False

User: \*\*\*\*\*  
Level: Users  
This site is maintained by IT-EM

**Figure 8.31: Information Security awareness test for computer ethics completed by the secretary**





## ISRA

Information Security Retrieval and Awareness Model



---

[Home](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Physical Security

- Physical Security is only man made threats.  
 True  
 False
- Fire safety should be part of the Physical Security Policy.  
 False  
 True
- It is important to ensure that no unauthorised people are able to access information.  
 False  
 True
- Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facility used to support their operation.  
 False  
 True
- Personal computers, laptops and personal digital assistants could pose a physical risk.  
 False  
 True
- Back-up procedures should be included in the Physical Security Policy.  
 False  
 True
- Physical Security is not part of the overall security policy.  
 True  
 False
- Employees, contractors and contractor employees should be briefed regularly on the physical security measures operating in their work environment.  
 True  
 False

9) Appropriate physical security and access control measures should be established for information technology.

True  
 False

10) Users should \_\_\_\_\_ the Physical Security Policy.

be committed to  
 ignore  
 take note of

11) It is advisable to write down your password on your desk pad.

False  
 True

12) Physical Security is about preventing access to information.

False  
 True

13) Physical Security is about protecting the computer system from \_\_\_\_\_.

people outside the organisation  
 all people  
 people inside the organisation

14) Physical security describes protection needed outside the computer system.

False  
 True

15) Physical Security controls the \_\_\_\_\_ of all stakeholders.


entry and exit  
 entry  
 exit

16) Physical Security is a \_\_\_\_\_ issue.

technical and non-technical  
 technical  
 non-technical


User: \*\*\*\*\*  
Level: Users

**Figure 8.32: Information Security awareness test for physical security completed by the secretary**



## ISRA

Information Security Retrieval and Awareness Model



---

[Home](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Security Policy

- Compliance Monitoring should be conducted \_\_\_\_\_.
  - whenever you remember
  - regularly
  - as soon as an Information Security incident occurs
  - once a year
- Users have the authority to change the Information Security Policy.
  - True
  - False
- Non-repudiation is \_\_\_\_\_.
  - ensuring that information is not disclosed to any unauthorised party
  - ensuring that no action that was taken and that affects Information Security can be denied at a later stage
  - determining whether or not the authenticated party has the right to access the information
  - ensuring that information is still in its original form and that no tampering or alteration has taken place
- Users should \_\_\_\_\_ the Information Security Policy.
  - take note of
  - be committed to
  - ignore
- Confidentiality is \_\_\_\_\_.
  - ensuring that information is not disclosed to any unauthorised party
  - ensuring that no action that was taken and that affects Information Security can be denied at a later stage
  - ensuring that information is still in its original form and that no tampering or alteration has taken place
- Top Management has the authority to change the Information Security Policy.
  - False
  - True
- An information policy should incorporate new technologies.
  - False
  - True
- A password should be \_\_\_\_\_.
  - complex
  - easy
  - short
  - only characters

Chapter 8

164

9) The Information Security Policy must be distributed to \_\_\_\_\_.

only new stakeholders  
 all stakeholders

10) A trapdoor is a \_\_\_\_\_.

code that makes information accessible to unauthorised  
 program that overly does one thing while covertly doing another  
 program that has secret entry points

11) Authorisation is \_\_\_\_\_.

ensuring that information is not disclosed to any unauthorised party  
 ensuring that no action that was taken and that affects Information Security can be denied at a later stage  
 determining whether or not the authenticated party has the right to access the information  
 ensuring that information is still in its original form and that no tampering or alteration has taken place

12) The Information Security Policy should consist of subpolicies.

True  
 False

13) The Security Policy should contain \_\_\_\_\_ on how to implement Information Security.

procedures  
 guidelines  
 processes, procedures and guidelines  
 processes

14) Integrity involves making sure \_\_\_\_\_.

that no action that was taken and that affects Information Security can be denied at a later stage  
 that information is not disclosed to any unauthorised party  
 whether or not the authenticated party has the right to access the information  
 that information is still in its original form and that no tampering or alteration has taken place

15) The Information Security Policy serves as the basis for establishing employees' accountability.

False  
 True

16) An information leak is a \_\_\_\_\_.

program that overly does one thing while covertly doing another  
 code that makes information accessible to unauthorised people  
 program that has secret entry points

User: \*\*\*\*\*  
Level: Users

This site is maintained by IT-EM

**Figure 8.33: Information Security awareness test for security policy completed by the secretary**

After the secretary had completed each test, the initial screen depicted in (Figure 8.27) was updated to reflect the result (see Figure 8.34).

The screenshot displays the ISRA web application interface. At the top left, there is a logo featuring a yellow padlock and the text 'ISRA Information Security Retrieval and Awareness Model'. To the right of the logo is a decorative graphic of a chain. Below the header is a navigation bar with links for 'Home', 'Information Security Awareness Program', 'Information Security Retrieval', and 'Log Out'. The main content area contains a table with the following data:


Information Security Issues relevant to your IT Authority Level		Date & Result of last test
<a href="#">Computer Ethics</a>	<a href="#">Do Test</a>	44% (2006/05/12)
<a href="#">Physical Security</a>	<a href="#">Do Test</a>	75% (2006/05/12)
<a href="#">Security Policy</a>	<a href="#">Do Test</a>	56% (2006/05/12)

Below the table is a 'Back' button. At the bottom left of the page, the following text is visible: 'User: \*\*\*\*\*', 'Level: Users', and 'This site is maintained by IT-EM'.

*Figure 8.34: Results for tests taken by the secretary*

The 'Date & Result of the last test' column in Figure 8.34 displays the result for each test, as well as the date on which the secretary completed each of the tests.

Next, the screens containing the tests completed by the accountant are displayed in Figures 8.35 to 8.37.



---

[Home](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Computer Ethics

- Ethics is a situational issue.  
 True  
 False
- Copyright is an ethical issue.  
 False  
 True
- There is \_\_\_\_\_ relationship between ethics and computer ethics  
 an indirect  
 no  
 direct
- Ethics can be seen as a set of prescribed rules or a code of behaviour that is to determine between \_\_\_\_\_.  
 all computers  
 all stakeholders
- Ethics is a set of \_\_\_\_\_.  
 rules set by law to determine what is right or wrong  
 principles based on religious rules and regulations  
 principles for justifying what is right or wrong
- Ethics is about honesty, fair play, proper compensation and respect for privacy.  
 False  
 True
- Ethical standards are \_\_\_\_ principles.  
 idealistic  
 legal  
 religious
- Ethics is a complex issue.  
 True  
 False

9) All stakeholders should understand what is meant by ethical behaviour.

True  
 False

10) There is always only one solution to ethical problems.

False  
 True

11) Adhering to a Code of Ethics is to do what is right and to \_\_\_\_\_ what is wrong.

report  
 disregard  
 ignore  
 disguise

12) Ethics should be part of the day-to-day activities of all employees.

True  
 False

13) It is unethical to download unauthorised software on your work computer.

False  
 True

14) Ethics is described as \_\_\_\_\_.

legislatures representing all people  
 unwritten principles  
 a formal, written document

15) Ethical principles are pre-identified problems.

False  
 True

16) Ethical conduct may influence your professional status.

True  
 False

User: \*\*\*\*\*  
Level: Users  
This site is maintained by IT-EM

**Figure 8.35: Information Security awareness test for computer ethics completed by the accountant**



## ISRA

Information Security Retrieval and Awareness Model



---

[Home](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Physical Security

- Physical Security is only man made threats.  
 True  
 False
- Fire safety should be part of the Physical Security Policy.  
 False  
 True
- It is important to ensure that no unauthorised people are able to access information.  
 False  
 True
- Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facility used to support their operation.  
 False  
 True
- Personal computers, laptops and personal digital assistants could pose a physical risk.  
 False  
 True
- Back-up procedures should be included in the Physical Security Policy.  
 False  
 True
- Physical Security is not part of the overall security policy.  
 True  
 False
- Employees, contractors and contractor employees should be briefed regularly on the physical security measures operating in their work environment.  
 True  
 False



9) Appropriate physical security and access control measures should be established for information technology.

True  
 False

10) Users should \_\_\_\_\_ the Physical Security Policy.

be committed to  
 ignore  
 take note of

11) It is advisable to write down your password on your desk pad.

False  
 True

12) Physical Security is about preventing access to information.

False  
 True

13) Physical Security is about protecting the computer system from \_\_\_\_\_.

people outside the organisation  
 all people  
 people inside the organisation

14) Physical security describes protection needed outside the computer system.

False  
 True

15) Physical Security controls the \_\_\_\_\_ of all stakeholders.


entry and exit  
 entry  
 exit

16) Physical Security is a \_\_\_\_\_ issue.

technical and non-technical  
 technical  
 non-technical


User: \*\*\*\*\*  
Level: Users  
This site is maintained by IT-EM

**Figure 8.36: Information Security awareness test for physical security completed by the accountant**



## ISRA

Information Security Retrieval and Awareness Model



---

[Home](#)   [Information Security Awareness Program](#)   [Information Security Retrieval](#)   [Log Out](#)

Please complete the assessment questions for Security Policy

- Compliance Monitoring should be conducted \_\_\_\_\_.
  - whenever you remember
  - regularly
  - as soon as an Information Security incident occurs
  - once a year
- Users have the authority to change the Information Security Policy.
  - True
  - False
- Non-repudiation is \_\_\_\_\_.
  - ensuring that information is not disclosed to any unauthorised party
  - ensuring that no action that was taken and that affects Information Security can be denied at a later stage
  - determining whether or not the authenticated party has the right to access the information
  - ensuring that information is still in its original form and that no tampering or alteration has taken place
- Users should \_\_\_\_\_ the Information Security Policy.
  - take note of
  - be committed to
  - ignore
- Confidentiality is \_\_\_\_\_.
  - ensuring that information is not disclosed to any unauthorised party
  - ensuring that no action that was taken and that affects Information Security can be denied at a later stage
  - ensuring that information is still in its original form and that no tampering or alteration has taken place
- Top Management has the authority to change the Information Security Policy.
  - False
  - True
- An information policy should incorporate new technologies.
  - False
  - True
- A password should be \_\_\_\_\_.
  - complex
  - easy
  - short
  - only characters

Chapter 8

171

9) The Information Security Policy must be distributed to \_\_\_\_\_.

only new stakeholders  
 all stakeholders

10) A trapdoor is a \_\_\_\_\_.

code that makes information accessible to unauthorised  
 program that overly does one thing while covertly doing another  
 program that has secret entry points

11) Authorisation is \_\_\_\_\_.

ensuring that information is not disclosed to any unauthorised party  
 ensuring that no action that was taken and that affects Information Security can be denied at a later stage  
 determining whether or not the authenticated party has the right to access the information  
 ensuring that information is still in its original form and that no tampering or alteration has taken place

12) The Information Security Policy should consist of subpolicies.

True  
 False

13) The Security Policy should contain \_\_\_\_\_ on how to implement Information Security.

procedures  
 guidelines  
 processes, procedures and guidelines  
 processes

14) Integrity involves making sure \_\_\_\_\_.

that no action that was taken and that affects Information Security can be denied at a later stage  
 that information is not disclosed to any unauthorised party  
 whether or not the authenticated party has the right to access the information  
 that information is still in its original form and that no tampering or alteration has taken place

15) The Information Security Policy serves as the basis for establishing employees' accountability.

False  
 True

16) An information leak is a \_\_\_\_\_.

program that overly does one thing while covertly doing another  
 code that makes information accessible to unauthorised people  
 program that has secret entry points

User: \*\*\*\*\*  
Level: Users  
This site is maintained by IT-EM

**Figure 8.37: Information Security awareness test for security policy completed by the accountant**

After the accountant had completed each test, the initial screen depicted in Figure 8.27 was updated to reflect the result - see Figure 8.38.

Information Security Issues relevant to your IT Authority Level	Do Test	Date & Result of last test
<a href="#">Computer Ethics</a>	Do Test	38% (2006/05/12)
<a href="#">Physical Security</a>	Do Test	75% (2006/05/12)
<a href="#">Security Policy</a>	Do Test	69% (2006/05/12)

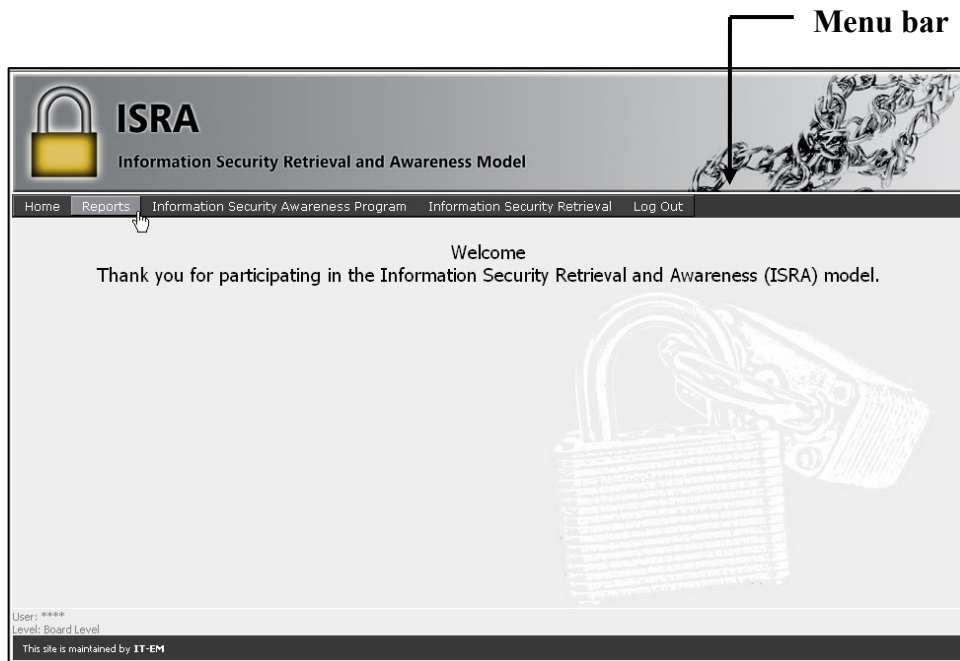
User: \*  
Level: Users  
This site is maintained by IT-EM

*Figure 8.38: Results for tests taken by accountant*

The 'Date & Result of the last test' column in Figure 8.38 displays the result for each test, as well as the date on which each test was completed by the accountant.

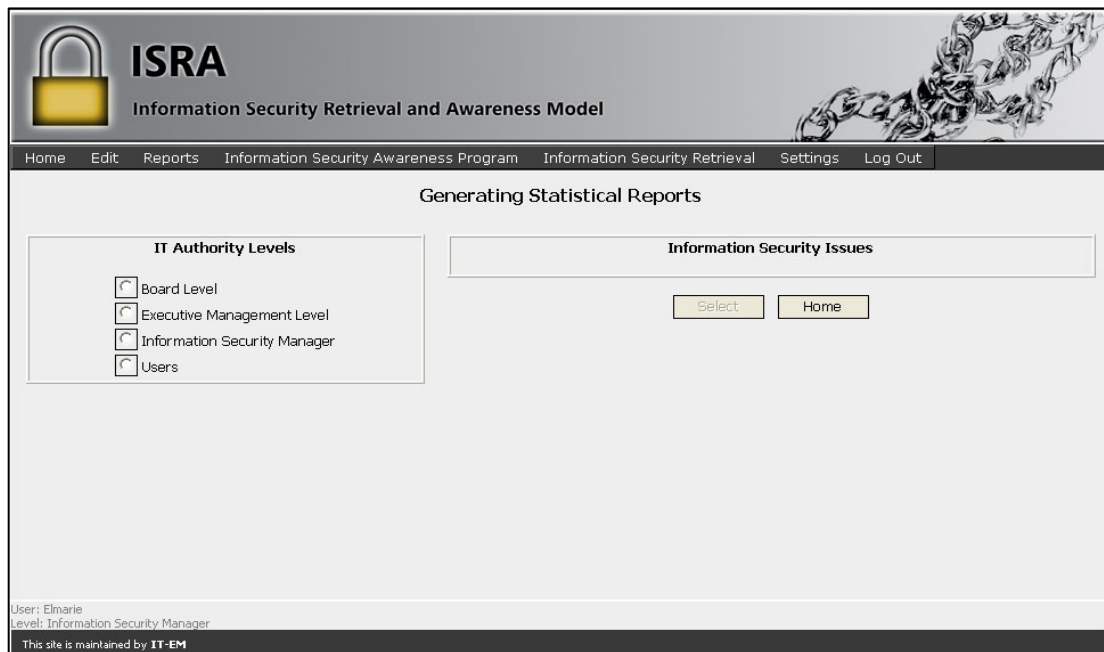
## 8.4.2 Reports

The second option selected by the owner was the Reports option on the menu bar, as depicted in Figure 8.39.



*Figure 8.39: Reports option*

The screen depicted in Figure 8.40 was displayed as a result.

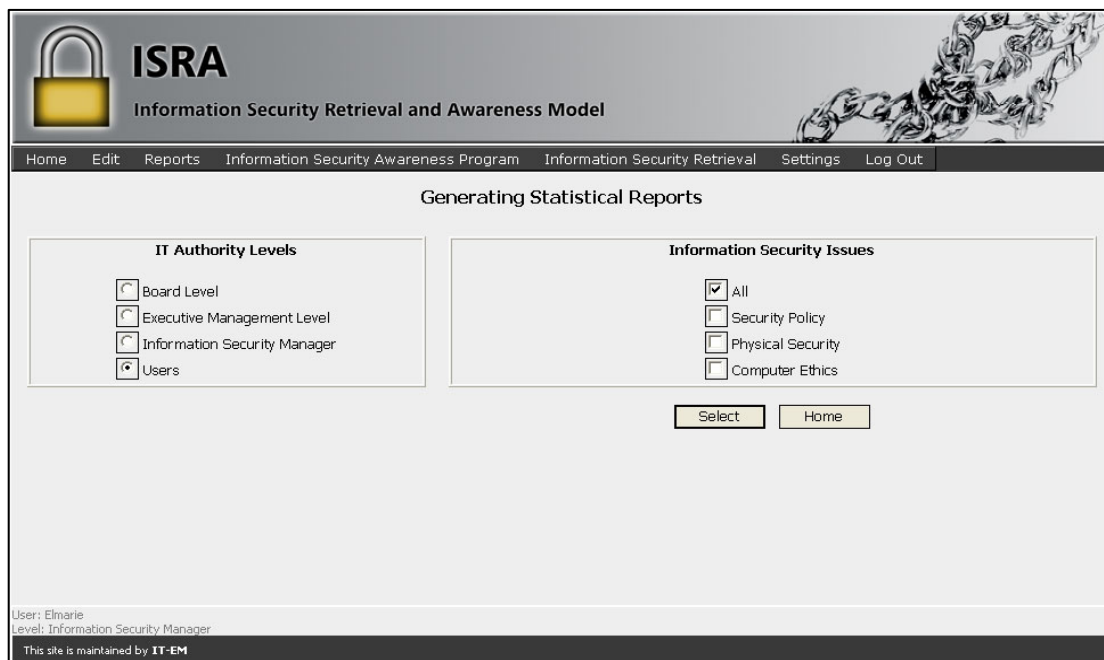


*Figure 8.40: Selecting the IT authority level for the report*

This option was also available to the partner, but partner decided not to make use of it. The Report option allows stakeholders (usually the Board and Executive Management level – unless access is granted to other stakeholders too) to extract statistical information

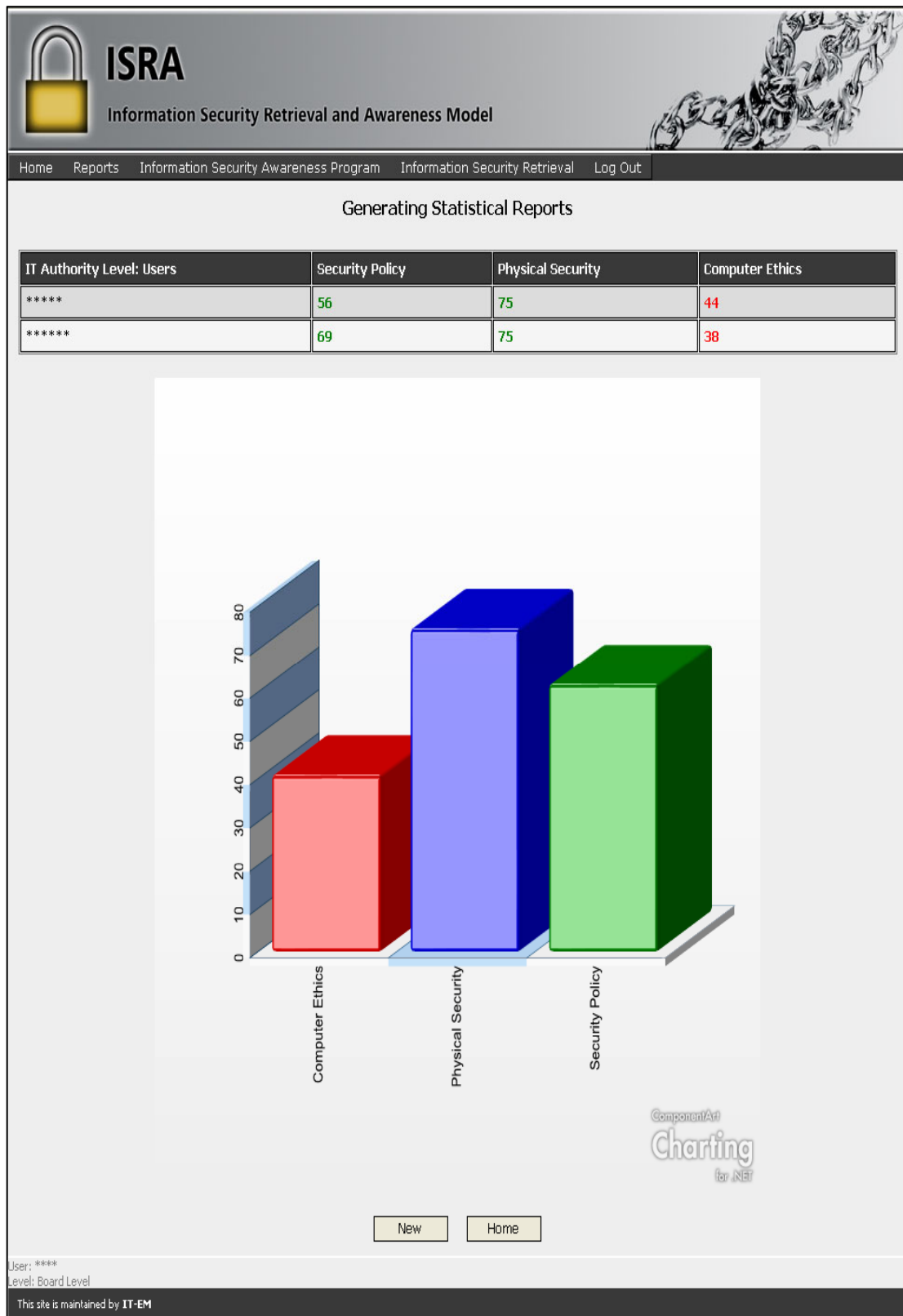
from the database to examine the Information Security awareness status within the organisation.

The screen depicted in Figure 8.40 displays a list of all IT authority levels present in Bekker & du Toit Optometrists (as well as the Information Security Management level). The owner wanted to determine the state of Information Security awareness among the **users**, and therefore selected 'Users' in the list of IT authority levels. The screen depicted in Figure 8.41 was displayed as a result.



*Figure 8.41: Selecting Information Security issues for the report*

This screen lists all the Information Security issues relevant to the User level. The owner wanted to determine the general status of Information Security awareness among the users and therefore selected the All option in the Information Security Issues list (thereby including all issues). The screen depicted in Figure 8.42 was displayed as a result.



**Figure 8.42: Report requested**

The report displayed in Figure 8.42 depicts the results (0%-100%) for each Information Security awareness test completed by the users (i.e. the secretary and the accountant).

The username of the users were disguised to protect their identity. The latest test result that each user obtained in respect of a specific Information Security issue is displayed in tabular format. If the test result was above 50%, it is indicated in green. If the test result was below 50%, it is indicated in red. The user whose information is displayed in the first row, for example, obtained 56% for the Information Security awareness test on security policy (indicated in green), 75% for the Information Security awareness test on physical security (indicated in green) and 44% for the Information Security awareness test on computer ethics (indicated in red).

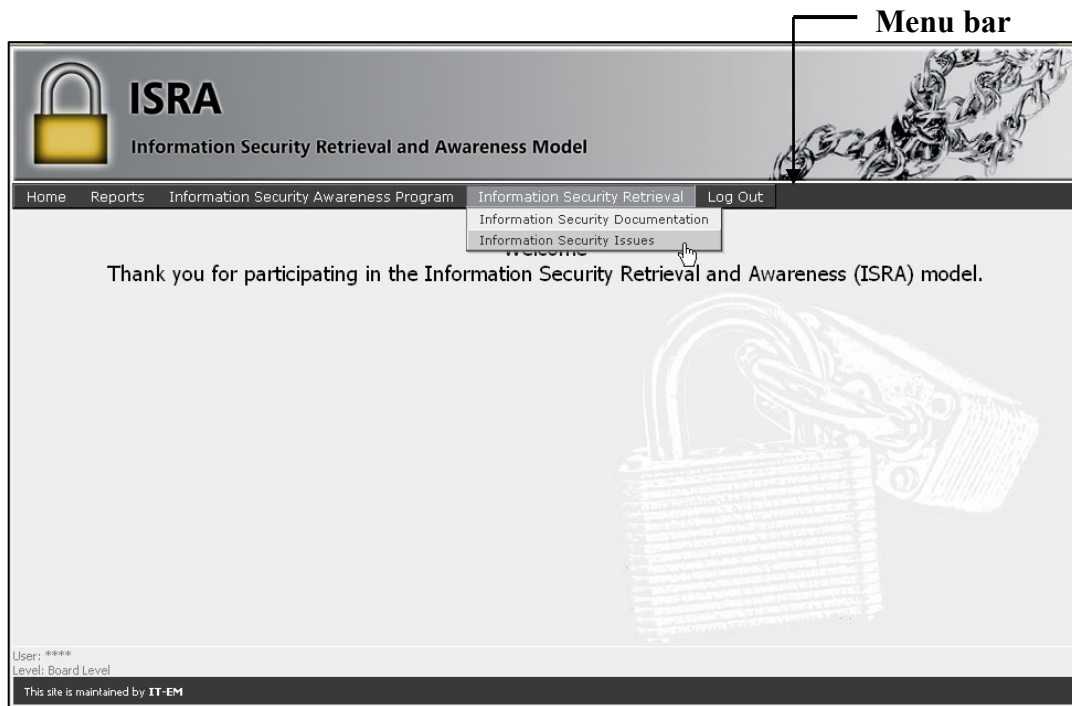
In addition, a summary of the test results is displayed in graphical format (i.e. bar chart). The bar chart depicted in Figure 8.42 displays the average test results regarding each Information Security issue. The average percentage (0%-100%) is depicted on the y-axis and the different Information Security issues are depicted on the x-axis. The average percentage of the two tests related to computer ethics – written by the secretary and the accountant respectively – is for example just above 40% (i.e. 41%). Based on this graphical representation, the owner concluded that the awareness of the users regarding computer ethics is poor and needs attention.

### 8.4.3 Information Security Retrieval

The last option selected by the owner was the Information Security Retrieval option on the menu bar. This option allows stakeholders to retrieve information directly from the database. It saves time and effort and no extra party needs to be involved. This option was also available to the partner, but the partner decided not to make use of it.

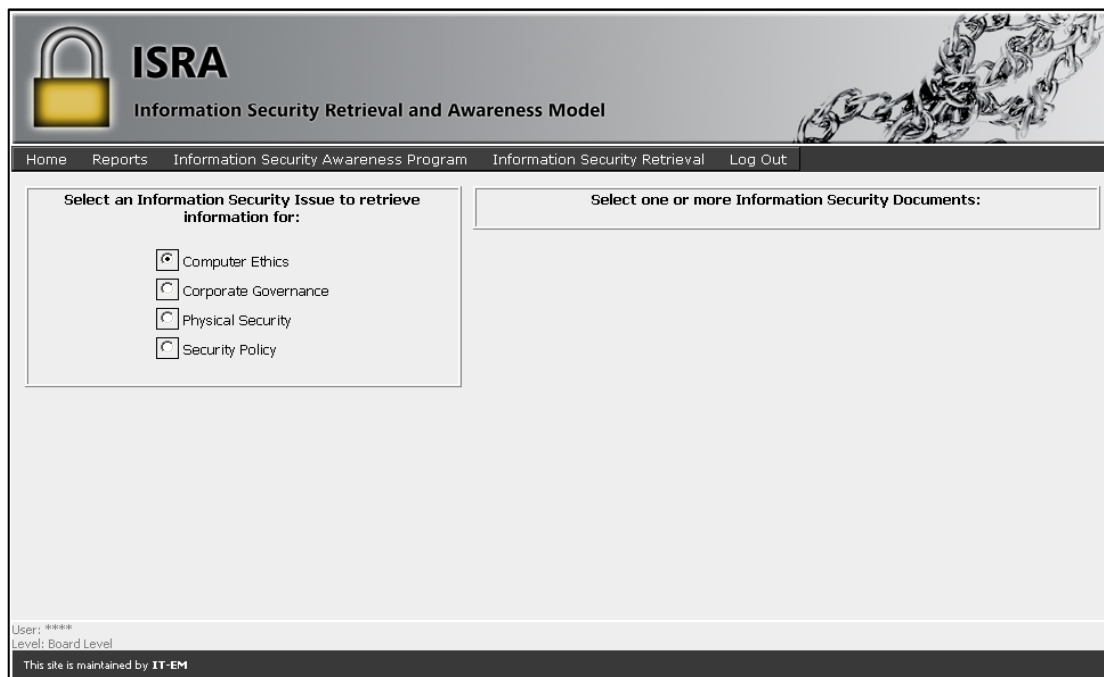
The owner decided to retrieve information regarding computer ethics on account of the low test results of the users in these issues (as depicted in Figure 8.42). The owner selected the Information on Information Security Issues option on the Information Security Retrieval menu option on the menu bar, as depicted in Figure 8.43.





**Figure 8.43: Information Security retrieval option**

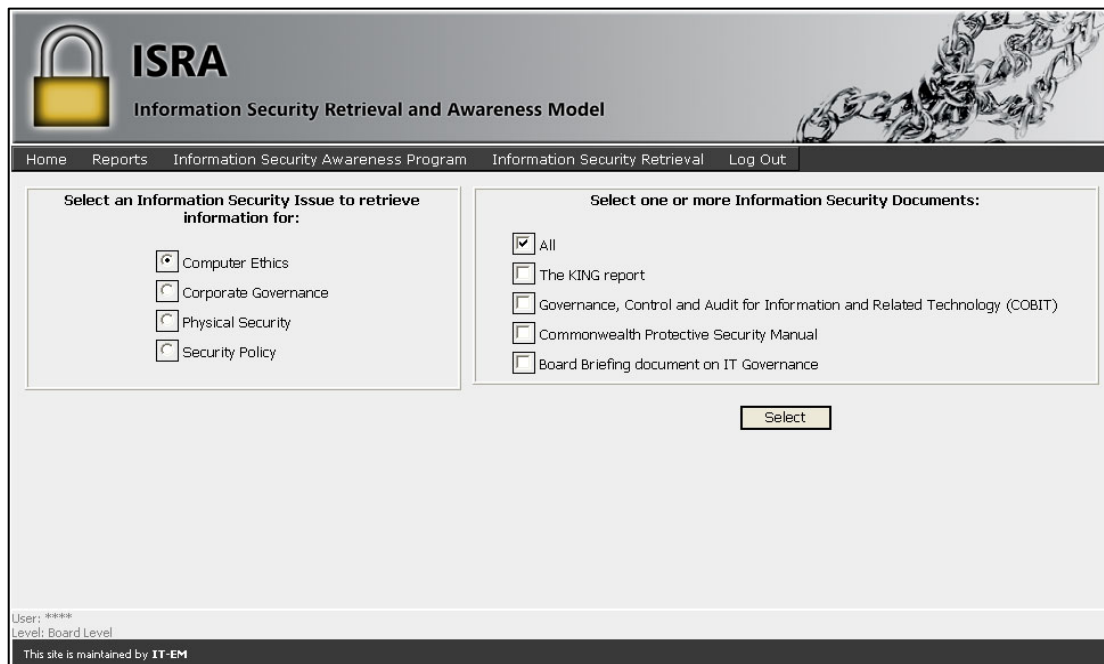
The screen that was displayed as a result is depicted in Figure 8.44.



**Figure 8.44: Selecting an Information Security issue for retrieval process**

This screen presents the owner with a list of all the non-technical Information Security issues related to the securing of information. The owner selected Computer Ethics

as the topic on which to retrieve more detailed information, and the screen depicted in Figure 8.45 was displayed as a result.



The screenshot shows the ISRA (Information Security Retrieval and Awareness Model) web application interface. The header includes the ISRA logo (a padlock) and the text "ISRA Information Security Retrieval and Awareness Model". A navigation menu contains links for "Home", "Reports", "Information Security Awareness Program", "Information Security Retrieval", and "Log Out".

The main content area is divided into two sections:

- Select an Information Security Issue to retrieve information for:**
  - Computer Ethics
  - Corporate Governance
  - Physical Security
  - Security Policy
- Select one or more Information Security Documents:**
  - All
  - The KING report
  - Governance, Control and Audit for Information and Related Technology (COBIT)
  - Commonwealth Protective Security Manual
  - Board Briefing document on IT Governance

A "Select" button is located below the document selection list. At the bottom left, the user information is displayed: "User: \*\*\*\*" and "Level: Board Level". The footer states "This site is maintained by IT-EM".

*Figure 8.45: Selecting one or more Information Security documents*

This screen depicts the different Information Security documents that address computer ethics in some way or another. The owner wanted to determine what information regarding computer ethics all the documents contained, and therefore selected the All option. The screen depicted in Figure 8.46 was displayed as a result.

The screenshot displays the ISRA (Information Security Retrieval and Awareness Model) web application. The header includes a logo with a padlock and the text 'ISRA Information Security Retrieval and Awareness Model'. A navigation bar contains links for 'Home', 'Reports', 'Information Security Awareness Program', 'Information Security Retrieval', and 'Log Out'. The main content area is titled 'Computer Ethics' and lists several documents with their respective IT Authority Levels:

- Board Briefing document on IT Governance**: IT Authority Level Involved: Users
- The KING report** (Empowered to support the enterprise's ethical principles...): IT Authority Level Involved: Information Security Manager, Users
- The KING report** (Establish the values of the enterprise...): IT Authority Level Involved: Board Level, Executive Management Level
- Commonwealth Protective Security Manual**: IT Authority Level Involved: Board Level, Executive Management Level
- Governance, Control and Audit for Information and Related Technology (COBIT)** (Management should create a framework...): IT Authority Level Involved: Board Level, Executive Management Level
- Governance, Control and Audit for Information and Related Technology (COBIT)** (Management should ensure that appropriate procedures...): IT Authority Level Involved: Board Level, Executive Management Level

At the bottom of the page, there is a 'Home' button, user information ('User: \*\*\*\*', 'Level: Board Level'), and a footer note: 'This site is maintained by IT-EM'.

**Figure 8.46: Results of retrieval process**

The above screen displays the results of the retrieval process, which included what the selected Information Security documents state about computer ethics. The results also included an indication of the IT authority level that should be aware of the information displayed.

### 8.5 Strengths and limitations of the prototype

All three parts of the ISRA model were incorporated in the prototype. However, a prototype is not meant to be a fully working system. The purpose of the prototype was to enhance Information Security awareness among the stakeholders and to provide them with the opportunity to retrieve relevant information directly from the database. The strengths of the prototype are listed below.

- The prototype is user-friendly.
- The prototype illustrates that the ISRA model can be implemented successfully.
- Each user is able to retrieve information regarding a specific Information Security issue at his/her own time and without having to involve another party.
- The database used in the prototype can be populated to suit the specific needs of an organisation, e.g. by adding IT authority levels as required.
- The reporting option enables top management to get a clear picture of the Information Security awareness status of IT authority levels (and specific stakeholders) at a glance.

The prototype does, however, also have the following limitations:

- The prototype incorporates a small range of security measures only. For example, all users should provide their correct username and password combination during the login process. Additional security measures could be added to the prototype, for example to prevent a user to login after three incorrect attempts.
- Although the prototype incorporates some validation measures (e.g. a user cannot delete information used somewhere else in the prototype), not all validation situations have been attended to.
- The prototype stores and displays only the latest Information Security awareness test results for each stakeholder. The prototype should be enhanced to include a history of test results (i.e. all test results for each stakeholder should be stored and not only the latest result). These test results could be used in the statistical report function to display the status of Information Security awareness over a period of time.
- The prototype does not provide detailed feedback to the users after they have taken an Information Security awareness test – it displays the percentage obtained only.

- The prototype incorporates only the first two slicing methods (i.e. y- and z-slicing) to retrieve information from the database. The third slicing method – combination slicing - was not included in the retrieval process.
- The prototype incorporates only one report option that displays the results of the requested information in a tabular and graphical format. The prototype could be expanded to include more report options.
- The execution of the application is slow if the stakeholders participate by using the Internet.

### 8.6 Conclusion

This chapter took a closer look at the prototype that was developed to implement the ISRA model. The prototype was implemented in a small real-life optometrist institution comprising of four stakeholders – grouped into three IT authority levels. All the stakeholders participated in the implementation phase of the prototype and found the prototype user-friendly and hence easy to use.

Both users (the secretary and the accountant) studied the information regarding each Information Security issue before they separately completed the Information Security awareness tests. The secretary did not comment on the test procedure, whereas the accountant commented that he had found the information provided by the prototype a big help in completing the tests.

The partner, on the other hand, did not study the information in detail but only glanced at it. The partner then continued and completed all four Information Security awareness tests without any comments.

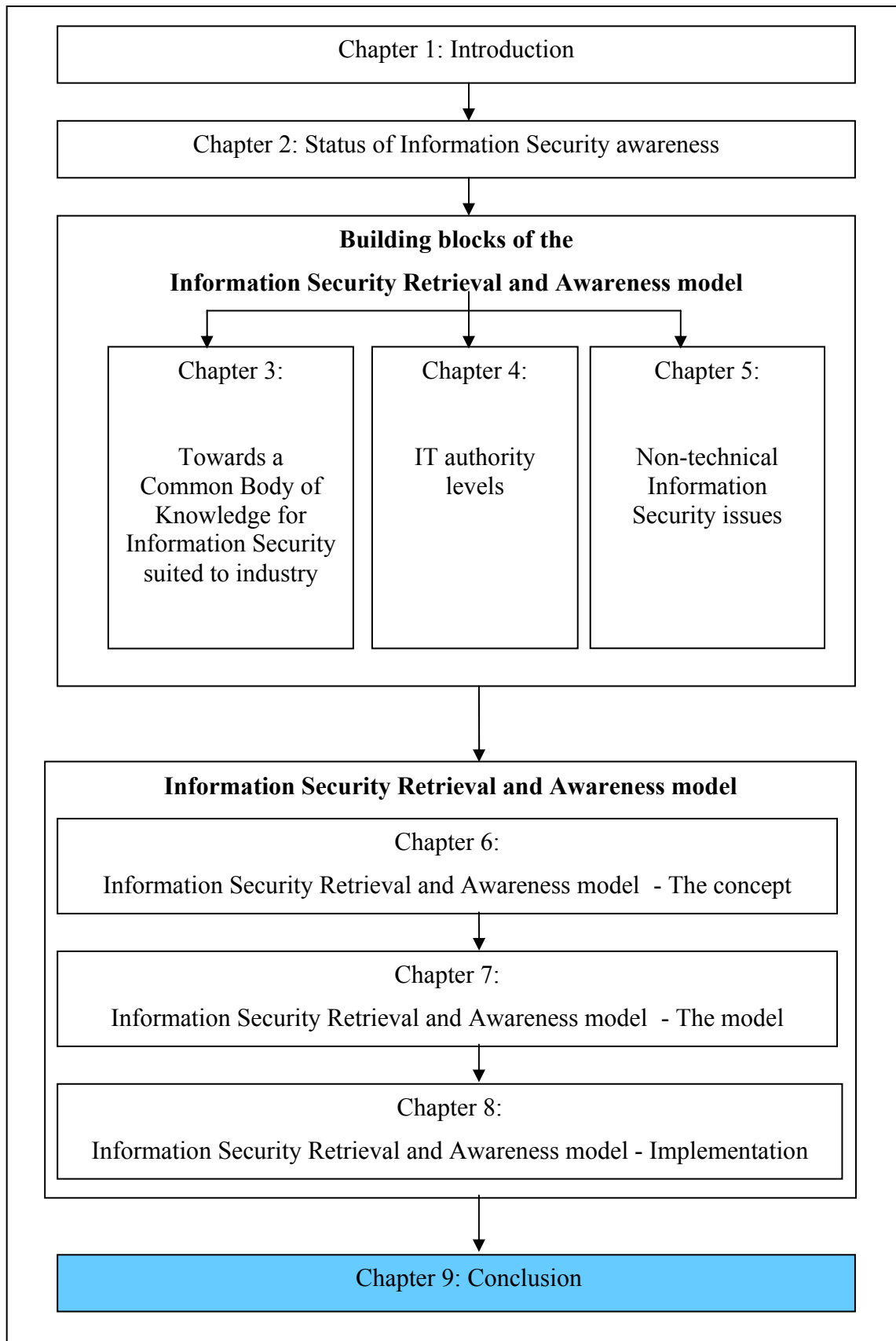
The owner, in turn, studied all relevant information in detail and completed the tests accordingly. The owner then decided to generate a report on the status of Information Security awareness among users. Having studied the results of the generated report – which included the average percentages of all three Information Security issues (i.e. computer ethics, security policy and physical security) – the owner diagnosed a general lack of knowledge regarding computer ethics among users. Due to the low average mark

gained for computer ethics, the owner requested detailed information from the database regarding computer ethics in all documents stored in the database.

The current thesis culminates in Chapter 9. In it, the author summarises the research undertaken and analyses the ISRA model to determine whether the research questions stipulated in Chapter 1 have been dealt with. The thesis is concluded with a reflection on possible areas for further research.

# **Chapter 9**

## **Conclusion**





## **9.1 Introduction**

Chapter 9 concludes with an overview of the research that was conducted within this thesis. The advantages and disadvantages of the Information Security Retrieval and Awareness (ISRA) model developed in this thesis are discussed, as well as the contribution of the ISRA model to Information Security awareness in industry.

The chapter also highlights future research work that could further enhance the current study.

## **9.2 Research overview**

The primary goal of this thesis was to make a contribution towards enhancing Information Security awareness among employees within the industry sector. In a bid to do so, the researcher set out to develop an Information Security retrieval and awareness model for industry. The problem statement derived from the goal is accordingly re-examined with a view to ascertaining the extent to which this had been accomplished.

### **9.2.1 What is the current status of Information Security awareness?**

The Information Security community comprises of three Information Security sectors, namely government, industry and academia. Each sector has a specific goal and emphasis in respect of Information Security awareness.

The primary aim of the government sector regarding Information Security awareness is to ensure that the information within a specific country is protected against Information Security threats and that information users are aware of Information Security laws and regulations in this regard. Governments from around the globe have initiated directives to enhance the overall Information Security awareness of various countries. However, due to the ever-evolving nature of Information Technology that causes new Information Security threats to surface, the government sector should aim to keep up with these developments by constantly seeking new initiatives to enhance the Information Security awareness in this sector.

Along the same line, Information Security awareness in the industry sector needs to be enhanced on a constant basis. The primary aim of industry regarding Information

Security awareness is to ensure that all stakeholders are aware of the rules and regulations aimed at securing the information they work with. Many organisations perceive Information Security as a purely technical issue and fail to pay attention to human-related Information Security issues. When aiming to enhance Information Security awareness in industry, the technical Information Security issues and the non-technical, human-related issues should receive an equal amount of attention. Furthermore, employees are often burdened with irrelevant information related to Information Security. It is the responsibility of top management to address these issues, but a lack of commitment is often noted in this regard.

More recently, the academic sector started to incorporate Information Security in their curricula. The primary goal of the academic sector regarding Information Security awareness is to provide learners with the skills and knowledge to prepare them for future occupations in some field that includes elements of Information Security. A number of tertiary institutions have not yet incorporated Information Security in their curricula, or have incorporated Information Security at postgraduate level only. Furthermore, Information Security is often restricted to the disciplines of Computer Science and Information Systems, whereas it should be integrated with other applicable study fields as well. Finally, Information Security curricula tend to put more emphasis on technical Information Security issues, while they should rather strike a balance between technical and non-technical Information Security issues. Additionally it should be ensured that the academic sector itself provide the necessary awareness and experience for its own staff to provide reliable information security education.

It can be concluded from this investigation that there is room for improvement in respect of Information Security awareness within all three Information Security sectors. However, the current thesis focused exclusively on enhancing Information Security awareness in the **industry** sector.

### **9.2.2 What is meant by non-technical, human-related Information Security issues?**

Information Security can be divided into technical and non-technical, human-related issues. The technical Information Security issues focus primarily on the technical

knowledge and tools required to secure information. On the other hand, the non-technical, human-related Information Security issues refer to the human-related knowledge required to secure information.

Many Information Security specialists focus on the technical Information Security issues only, because these issues have been around since the early 1960s, whereas the non-technical, human-related Information Security issues emerged around the middle 1980s only. Organisations should, however, aim to strike a balance between the technical Information Security issues and the non-technical, human-related Information Security issues. This research identified the current non-technical, human-related Information Security issues to be risk management, Information Security management, legal issues, computer ethics, professionalism, Information Security culture, Information Security policies and physical security. The ISRA model focuses only on these non-technical Information Security issues, because of the lack of attention they currently receive in industry.

### **9.2.3 What Information Security issues should employees be aware of to enhance Information Security awareness?**

There are currently numerous state-of-the-art Information Security documents that could be used as guidelines by organisations on how to protect their information. These documents include vast amounts of information on Information Security issues that employees should be aware of in their day-to-day activities.

The author identified and investigated ten such state-of-the-art Information Security documents. These documents were used as a basis to propose a Common Body of Knowledge for Information Security suited to industry. The proposed Body of Knowledge was divided into technical Information Security issues and non-technical Information Security issues. It contains information on Information Security that stakeholders should be aware of in industry. It should be kept up to date by incorporating new Information Security documents whenever required and by removing or updating documents whenever outdated.

### **9.2.4 How can one prevent employees from being burdened with unnecessary information?**

Many stakeholders within industry are already weighed down with work-related issues. Organisations should therefore ensure that they do not add unnecessary information to their stakeholders' already overflowing work responsibilities. This could result in a situation where stakeholders will avoid participating in Information Security awareness programmes, because they do not have the time to study piles of information of which a great part might be irrelevant to their job category. To prevent employees from being troubled with irrelevant information, stakeholders were grouped into IT authority levels according to job category, and were accordingly assigned with different roles and responsibility towards securing information.

The different IT authority levels will differ from one organisation to the next depending on their Information Security needs and structure. For the purpose of this thesis, the IT authority levels in a typical organisation were identified as the Board level, Executive Management level, Middle Management level, Information Security Management level, Technical Management level and the User level. Each IT authority level needs to be aware only of those Information Security issues (in the proposed Common Body of Knowledge) that are pertinent to their particular level.

## **9.3 Pros and cons of the ISRA model**

The proposed Information Security Retrieval and Awareness (ISRA) model for industry obviously has certain pros and cons, which will be discussed next.

The advantages of the model are that it will enhance Information Security awareness in the said domain in the following manner:

- The ISRA model is based on a Common Body of Knowledge for Information Security specifically suited to industry. This Common Body of Knowledge draws a clear distinction between technical Information Security issues and non-technical Information Security issues.
- The ISRA model focuses on the non-technical, human-related Information Security issues within industry. Seeing that research into the technical issues has been around since the 1950s and virtually all Information Security models focus

primarily on these issues, the non-technical, human-related Information Security issues have been largely overlooked or ignored.

- The ISRA model does not only focus on Information Security professionals, but ensures that all stakeholders in an organisation (including users with little or no Information Security knowledge and experience) are part of the Information Security awareness process. This is achieved through assigning all stakeholders to a specific IT authority level within an organisation.
- In addition, the ISRA model ensures that stakeholders are made aware of the non-technical, human-related Information Security issues related to their job category only, preventing them from being troubled with unnecessary information. This is achieved by assigning different information security responsibilities to each IT authority level.
- Finally, the ISRA model incorporates a retrieval component, which will allow stakeholders to retrieve specific information related to Information Security issues at any time and without involving another party. The purpose of such a retrieval process is to enhance the Information Security awareness of the stakeholders.

However, the proposed model suffers from the following limitations.

- The ISRA model focuses on enhancing Information Security Awareness in the industry sector only – the government and academic sectors do not form part of the scope of the model. It can therefore not be used for these two sectors without the necessary adaptations.
- Although the ISRA model uses the proposed Common Body of Knowledge for Information Security suited to industry as a building block, it focuses on the non-technical, human-related Information Security issues that form part of this Common Body of Knowledge.
- When designing Information Security awareness programmes, factors such as human behaviour should also be taken into account. However, this was not part of the scope of the ISRA model.

## 9.4 Future research

This thesis provides a fresh approach towards enhancing Information Security awareness in the industry sector. The limitations highlighted in the previous paragraph nevertheless uncover potential areas for future research.

The ISRA model was primarily designed for use in industry. Further research should therefore be conducted to investigate how such a model could be adapted to meet the Information Security awareness needs in the government and academic sectors.

Another area that will benefit from further research concerns ways in which the ISRA model could be expanded to include the technical Information Security issues as well.

Finally, the measuring part of the ISRA model should be investigated further with a view to identifying those factors that should play a role in the development of such tests.

# References

- Aljifri, H. & Navarro, D.S. (2003). International legal aspects of cryptography, *Computers & Security*, 22(3): 196-203.
- Allinson, C. (2001). Information Systems Audit Trails in Legal Proceedings as Evidence, *Computers & Security*, 20(5): 409-421.
- Andersen, P.W. (2001). Information Security Governance, *Information Security Technical Report*, 6(3): 60-70.
- Anderson, J.M. (2003). Why we need a new definition of information security, *Computers & Security*, 22(4): 308-313.
- Armstrong, H. & Jayaratna, N. (2002). Internet Security Management: A Joint Postgraduate Curriculum Design, *Journal of Information Systems Education*, 13(3): 249-258.
- Attorney General's Department (2000). *Commonwealth Protective Security Manual*, Commonwealth of Australia. Accessed on 20/04/2005. Available at: [http://www.dsd.gov.au/lib/pdf\\_doc/acsi33/ACSI33\\_U\\_0304.pdf](http://www.dsd.gov.au/lib/pdf_doc/acsi33/ACSI33_U_0304.pdf).
- Bacon, T. & Tikekar, R. (2003). Experiences with developing a computer security information assurance curriculum, *Journal of Computing Sciences in Colleges*, 18(4): 254-267.
- Bauknight, T.Z. (2005). The Newest Internet Scams, *Business and Economic Review*, 52(1): 19-21.
- Becker, D. (2004). *MyDoom virus declared worst ever*, Accessed on 04/03/2005. Available at: [http://news.zdnet.com/2100-1009\\_22-5149764.html](http://news.zdnet.com/2100-1009_22-5149764.html)
- Berinato, S. (2005). *The Global State of Information Security*, CIO Magazine, 15 September, Accessed on 05/06/2005. Available at: [www.cio.com](http://www.cio.com).
- Bessagnet, M., Schlenker, L., Aiken, R. & Laforcade, P. (2005). Can collaborative technologies improve management education, in *Proceedings of the Fifth International Conference on Advanced Learning Technologies (ICALT)*. 233-234.
- Bishop, M. (2000a). Education in information security, *IEEE Concurrency*: 8(4).
- Bishop, M. (2000b). Academia and Education in Information Security: Four Years later, in *Proceedings of the Fourth National Colloquium on Information System Security Education. (Keynote address)*.
- Bishop, M. & Frincke, D. (2005a). *A Human Endeavour: Lessons from Shakespeare and Beyond*, *IEEE security & privacy*, 3(4), 49-51.
- Bishop, M. & Frincke, D. (2005b). *Teaching Secure Programming*, *IEEE security & privacy*, 3(5), 54-56.



- Bogolea, B. & Wijekumar, K. (2004). Information Security Curriculum Creation: A Case Study, in *Proceedings of the 1st annual conference on Information security curriculum development*. 59-65.
- Briney, A. (2003). *Law and order*, Information Security, Accessed on 28/01/2005.  
Available at:  
[http://infosecuritymag.techtarget.com/articles/august00/columns5\\_logoff.shtml](http://infosecuritymag.techtarget.com/articles/august00/columns5_logoff.shtml).
- Briney, A. (2004). *10 Laws of security*, Information Security, Accessed on 28/02/2005.  
Available at:  
[http://infosecuritymag.techtarget.com/articles/august00/columns5\\_logoff.shtml](http://infosecuritymag.techtarget.com/articles/august00/columns5_logoff.shtml).
- British Standards Institute - BSI (2002). Information security management system - specifications with guidance for use, final draft BS7799-2:2002.
- Broderick, J.S. (2001). Information Security Risk Management - When should it be Managed? *Information Security Technical Report*, 6(3): 12-18.
- Burnett, R. (2005). Legal risk management for the IT industry, *Computer Law & Security Report*, 21(1): 61-67.
- Cadbury Report (1992). *Report of the committee on the Financial Aspects of Corporate Governance*, Gee, London, United Kingdom.
- CCTA (1999). *IT Infrastructure Library on Security Management document*. Crown, Norwhich.
- Chandler, H.E. (1998). Towards open government: official information on the Web, *New Library World*, 99(6): 230-237.
- CIO & PriceWaterhouseCoopers (2005). *The Global State of Information Security*, CIO Magazine, 15 September, Accessed on 04/12/2005. Available at: [www.cio.com](http://www.cio.com).
- Clarke, T. (1998). The contribution of non-executive directors to the effectiveness of corporate governance, *Career Development International*, 3(3): 118-124.
- COBIT (2001). *Governance, Control and Audit for Information and Related technology (COBIT)*, IT Governance Institute, ISACA, ISACF, 3rd edition, 2001, ISBN 1-893209-13-X.
- Cockcroft, S. (2002). Securing the commercial Internet: Lessons learned in developing a postgraduate course in information security management, *Journal of Information Systems Education*, 13(3): 205-210.
- Colloquium for Information Systems Security Education - Asia-Pacific (CISSE-AP). Accessed on 14/09/2006. Available at: <http://www.cisse-ap.org.au/>

- Committee of the Financial Aspects of Corporate Governance (1992). *The Financial Aspects of Corporate Governance*, Burgess Science Press, Great Britain.
- Committee on National Security Systems - CNSS (2006), Accessed on 14/09/2006. Available at: <http://www.cnss.gov/instructions.html>
- CompTIA (2006). *Fourth annual CompTIA study on information security and the workforce*, Accessed on 05/04/2006. Available at: [http://www.comptia.org/about/pressroom/get\\_pr.aspx?prid=903](http://www.comptia.org/about/pressroom/get_pr.aspx?prid=903).
- Corporate Governance Task Force Report (2004). *Information Security Governance: A call to action*, Accessed on 02/03/2005. Available at: <http://www.isacaroma.it/html/newsletter/?q=node/45>.
- Crowley, E. (2003). Information Systems Security Curricula Development, in *Proceedings of the 4th conference on IT curriculum on IT Education*.
- CSI/FBI (2005). *Computer Crime and Security Survey*, Available at: GoCSI.com.
- Cutler, K. (2000). *Hitting the Bull's eye*, Accessed on 06/07/2005. Accessed on 16/04/2005. Available at: [http://infosecurymag.techtarget.com/articles/august00/columns5\\_logoff.shtml](http://infosecurymag.techtarget.com/articles/august00/columns5_logoff.shtml).
- Danchev, D. (2003). *Reducing Human Factor Mistakes*, Accessed on 05/03/2005. Available at: <http://www.windowsecurity.com>.
- Das Bundesamt für Sicherheit in der Informationstechni - BSI (2002). *Secure information technology for our society*, Accessed on 02/01/2005. Available at: <http://www.bsi.de/english/index.htm>.
- Deloitte, Touche & Tohmatsu (2005). *Global Security Survey*, Accessed on 11/012/2005. Available at: [www.deloitte.com](http://www.deloitte.com).
- Dhillon, G. & Moores, S. (2001). Computer crimes: theorizing about the enemy within, *Computers & Security*, 20(8): 715-723.
- Doherty, N.F. & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan, *Computers & Security*, 25(1): 55-63.
- Dwan, B. (2001). Something new, Something old, *Computer Fraud & Security*, (9): 7.
- Edwards, M.J. (2003). *The Legal liability of Information Security*, Accessed on 24/2/2005. Available at: [www.windowstpro.com/Article/ArticleID/38846/38846/38846.html](http://www.windowstpro.com/Article/ArticleID/38846/38846/38846.html).
- Eloff, J.H.P. & Eloff, M.M. (2005). Information Security Architecture, *Computer Fraud & Security*, (11): 10-16.

- Ernest & Young (2003). *Global Information Security Survey*, Accessed on 17/03/2005. Available at: <http://www.ey.com>.
- Ernest & Young (2004). *Global Information Security Survey*, Accessed on 17/03/2005. Available at: <http://www.ey.com>.
- F-Secure (2004). *F-Secure Corporation's Data Security Summary for 2004*, Accessed on 02/03/2005. Available at: <http://www.f-secure.com>.
- Finne, T. (2000). Information Systems Risk Management: Key Concepts and Business Processes, *Computers & Security*, 19(3): 234-242.
- Fisher, U. (2001). *Information Age State Security: New Threats to Old Boundaries*, Accessed on 02/11/2004. Available at: [www.homelandsecurity.org/journal/articles/fisher.htm](http://www.homelandsecurity.org/journal/articles/fisher.htm).
- Floridi, L. (2005). Information ethics, its nature and scope, *ACM SIGCAS Computers and Society*, 35(2).
- Fonseca, B. (2000). *Manage people to protect data*, Accessed on 04/01/2005. Available at: <http://www.infoworld.com/articles/hn/xml/00/11/13/001113hncorporate.html>
- Forcht, K.A. (1994). *Computer Security Management*, Boyd & Fraser, United States of America.
- Fotinger, C.S. & Ziegler, W. (2004). Understanding a hacker's mind - A psychological insight into the hijacking of identities, *A White Paper by the Danube-University*, Zentrum für praxisorientierte Informatik, Dr Karl-Dorrek Strabe 30, A-3500 Krems.
- Fraser, H.S.F., Kohane, I.S. & Long, W.L. (1997). *Using the technology of the world wide web to manage clinical information*, Accessed on 24/12/2004. Available at: <http://bmj.bmjournals.com/archive/7094ip1.htm>.
- Fumy, W. (2004). It security standardization, *Network Security*, 12:6-11.
- Furnell, S.M., Gennatou, M. & Dowland, P.S. (2002). A prototype tool for information security awareness and training, *Logistics Information Management*, 15(5/6): 352-357.
- Gallivan, M. & Srite, M. (2005). Information technology and culture: Identifying fragmentary and holistic perspectives of culture, *Information and Organization*, 15(4): 295-338.
- Gamma (1999). *BS 7799*, Accessed on 02/03/2005. Available at: [www.gammasl.co.uk](http://www.gammasl.co.uk).
- Gerber, M. & Von Solms, R. (2005). Management of risk in the information age, *Computers & Security*, 24(1): 16-30.

- Gincel, R. (2004). *Are you ready for the feds?* Available at: [http://www.infoworld.com/article/04/08/06/32FEcomply\\_1.html?s=feature](http://www.infoworld.com/article/04/08/06/32FEcomply_1.html?s=feature)
- GMITS (2001). *GMITS: Guidelines for the Management of IT Security, Part 1: Concepts and models for managing and planning IT security*, ISO/IEC JTC1/SC27, PDTR 13335-1 (revision), version 28-11-2001.
- Gritzalis, D., Theoharidou, M. & Kalimeri, E. (2005). Towards an interdisciplinary information security education model, in *Proceedings of WISE4*, Moscow, Russia, pp. 22-35.
- Guant, N. (2000). Practical approaches to creating a security culture, *International Journal of Medical Informatics*, 60(2): 151-157.
- Hansche, S.H. (2001). *Information System Security Training: Making it Happen*, Accessed on 29/03/2005. Available at: [http://www.itknowledgebase.net/eJournals/articles/article\\_synopsis.asp?id=31727](http://www.itknowledgebase.net/eJournals/articles/article_synopsis.asp?id=31727)
- Heracleous, L. & Luh Luh, L. (2002). Who wants to be a competent director? *Corporate Governance: International Journal of Business in Society*, 2(4): 17-23.
- Hesse, L. & Smith, C.I. (1999). Core Curriculum in Security Science, in *Proceedings of the TC 11.8 Second World Conference on Information Security Education*, Australia.
- Hillburn, T.B. e. a. (1999). *A Software Engineering Body of Knowledge Version 1.0*, Software Engineering Institute, Pittsburgh, United States of America.
- Hoffman, T. (2006). *Q&A: Health care standards on the Table*, Accessed on 05/05/2006. Available at: <http://www.computerworld.com/databasetopics/data/story/0,10801,109417,00.html>.
- Hone, K. & Eloff, J.H.P. (2002). What makes an Effective Information Security policy, *Network Security*, (6): 14-16.
- Hulme, G.V. (2005). Data Breaches: Turn Back The Tide, *Business Credit*, 107(9): 34-39.
- IAA, AICPA, ISACA & NACD (2000). *A Call to action for Corporate Governance: Guidance for Boards of Directors*.
- Information Systems Audit and Control Association, (2006). Accessed on 15/09/2006. Available at <http://www.isaca.org/>.
- Information Week (2004). *2004 Global Information Security Survey*, Accessed on 27/02/2005. Available at:

- <http://www.informationweek.com/reports/showReport.jhtml?articleID=22103096>
- International Federation of Accountants (2000). *Managing Security of Information*.
- International Information Systems Security Certification Consortium (ISC)<sup>2</sup>, (2006). Accessed on 15/09/2006. Available at <https://www.isc2.org/cgi-bin/index.cgi>.
- Irvine, C.E., Chin, S.C. & Frincke, D. (1998). Integrating Security into Curriculum, *Computer*: 25-30.
- ISO 17799 Newsletter (2006). *ISO 17799 2005 Published*, Accessed on 28/04/2006. Available at: <http://17799-news.the-hamster.com/breaking-news-1.htm>.
- ISO/IEC177799 (2000). Information security Management – Part 1: Code of Practice for information security management. South African Bureau of Standards, South Africa.
- IT Governance Institute (2001a). *Information Security Governance: Guidance for Boards of Directors and Executive Management*, ISBN 1-893209-27-X.
- IT Governance Institute (2001b). *Board Briefing on IT Governance*, ISBN 1-893209-27-X.
- Johnson, J.D. (2000). *Presenting security awareness training at your company*, Accessed on 19/02/2005. Available at: <http://www.nwfusion.com>.
- Katsikas, S.K. (2000). A postgraduate Programme on Information and Communication System Security, in *Conference proceedings of the sixteen Annual working conference on Information Security*, 49-58. China.
- Katzke, S. (2001). *Security Metric*, Accessed on 20/04/2005. Available at: [http://72.14.209.104/search?q=cache:0uBifT0-mTsJ:www.cs.msstate.edu/~ia/IA\\_PAPERS/Katzke.pdf+security+metrics+katzke&hl=en&gl=za&ct=clnk&cd=3](http://72.14.209.104/search?q=cache:0uBifT0-mTsJ:www.cs.msstate.edu/~ia/IA_PAPERS/Katzke.pdf+security+metrics+katzke&hl=en&gl=za&ct=clnk&cd=3)
- King Report (2001). *The Code of Corporate Practices and Conduct*, Institute of Directors, South Africa.
- King Report (2002). *The Code of Corporate Practices and Conduct*, Institute of Directors, South Africa.
- Kisin, R. (1996). IT Security - Implementing "best practice", *Computer Audit Update*, (1): 9-21.
- Kritzinger, E. & Strous, L.A.M. (2002). Information Security: A Corporate Governance Issue, in *Proceedings of the fifth working Conference on Integrity and Internal Control in Information Systems*, 115-133. Bonn, Germany.

- Kritzinger, E. & Von Solms, S.H. (2004). The NOKIS Model, in *Proceedings of the 10th International Conference on information Systems analysis and synthesis*, Orlando, United States of America.
- Kwok, L. & Longley, D. (1997). Code of Practice: A Standard for Information Security Management., in *Proceedings of IFIP TC11, 13th International Conference on Information Security*.
- Kwok, L. & Longley, D. (1999). Information Security Management and modelling, *Information Management and Computer Security*, 7(1): 30-40.
- Laing, D. & Weir, C.M. (1999). Governance structure, size and corporate performance in UK firms, *Management Decision*, 37(5): 457-464.
- Le Grand, C. & Ozier, W. (2000). *Information Security Management Elements*, Accessed on 18/01/2005. Available at: <http://www.theia.org/itaudit/index.cfm?fuseaction=forum&fid=123>.
- Leach, J. (2003). Improving user security behaviour, *Computers & Security*, 22(8): 685-670.
- Lewis, A. (2000). Time to elevate IT security to the boardroom, *e Secure*, 1(1): 28.
- Lewis, R. (2003). The need for an Established Security Awareness Training Program, *SANS Institute*, July 10.
- Lindup, K. (1996). The role of information security in corporate governance, *Computers & Security*, 15(6): 477-485.
- Little, J.C., Granger, M.J., Boyle, R., Gerhardt-Powals, J., Impagliazzo, J., Janik, C., Kubilus, N.J., Lippert, S.K., McCracken, W.M., Paliwoda, G. & Soja, P. (1999). Integrating Professionalism and Workplace issues into the Computing and Information Technology Curriculum, *ITiCSE'99 Working Group Reports*, 31(4).
- Maner, W. (1996). Is computer ethics unique? *Science and Engineering Ethics*, 2(2): 137-154.
- Margulius, D. (2004). *Taking a page from ITIL's best practices*, Accessed on 15/04/2005. Available at: [http://www.infoworld.com/article/04/09/24/39FEitil\\_1.html](http://www.infoworld.com/article/04/09/24/39FEitil_1.html).
- Martins, A. & Eloff, J.H.P. (2002). Information Security Culture, in *Proceedings of IFIP SEC 2002, May 2002, Cairo, Egypt*.
- Martins, A. & Eloff, J.H.P. (2001). Measuring Information Security, in *Proceedings of the 1st annual ISSA Conference*, Johannesburg, South Africa.
- McConnell International (2000). *Cyber Crime...and Punishment?* Accessed on 09/01/2005. Available at: <http://www.mcconnellinternational.com>.

- McCoy, C. & Fowler, R.T. (2004). "You are the key to Security": Establishing a successful security awareness program, in *Proceedings of the 32nd annual ACM SIGUCCS conference on user services*, Baltimore, United States of America, pp. 346-349.
- McKay, J. (2003). Pitching the policy: implementing IT Security Policy through awareness, *SANS Institute*: 29-32.
- META Group (2000). *Service Management Strategies*, Accessed on 12/11/2004. Available at: [www.metagroup.com](http://www.metagroup.com).
- Minihan, K.A. (1998). *Defending the nation against cyber attack: Information Assurance in the global environment*, Accessed on 05/02/2005. Accessed on 23/03/2005. Available at: <http://usinfo.state.gov/journals/itps/1198/ijpe/pj48min.htm>.
- Morneau, K.A. (2004). Designing an information security program as a core competency of network technologists, in *Proceedings of the 5th conference on Information technology education*, Salt Lake City, United States of America.
- Morwood, G. (1998). Business continuity: awareness and training programmes, *Information Management & Computer Security*, 6(1): 28-32.
- Moulton, R. & Coles, R.S. (2003). Applying information security governance, *Computers & Security*, 22(7): 580-584.
- National Institute of Standards and Technology (2000). *An Introduction to Computer Security: The NIST Handbook.*, Special Publication 800-12. United States Dept. of Commerce, Technology Administration, National Institute of Standards and technology, United States.
- National Security Agency (2006). *Education and Training*, Accessed on 04/05/2005. Available at: <http://www.nsa.gov/about/about00005.cfm>.
- National Colloquium for Information Systems Security Education (NCISSE, 2006) Accessed on 14/09/2006, Available at: <http://www.cisse.info/>
- Ngo, L. & Zhou, W. (2005). The Multifaceted and Ever-Changing Directions of Information Security -Australia get ready, in *Proceedings of the Third International Conference on Information Technology and Application (ICITA'05)*.
- Nosworthy, J.D. (2000). Implementing Information Security in the 21<sup>st</sup> Century — Do You Have the Balancing Factors? *Computers & Security*, 19(4): 337-347.
- Palmer, M.E. (2001). Information Security Policy Framework: Best Practices for Security Policy in the E-Commerce age, *Information Systems Security*, 10(2): 13-27

- Pass, C. (2004). Corporate governance and the role of non-executive directors in large UK companies: an empirical study, *Corporate Governance*, 4(2): 52-63.
- Peltier, T. (2005). Implementing an Information Security Awareness Program, *Security Management Practices*: 37-48. Accessed on 12/09/2005. Available at: [http://www.itknowledgebase.net/eJournals/articles/article\\_synopsis.asp?id=89329](http://www.itknowledgebase.net/eJournals/articles/article_synopsis.asp?id=89329)
- Pfleeger, C.P. (1997). *Security in Computing*, Second ed, Prentice Hall, United States of America.
- Pfleeger, C.P. (2003). *Security in Computing*, Prentice Hall. Upper Saddle River, N.J.
- Pillay, K. (2000). Repositioning the private sector security industry in South Africa in the 21st century - the need for professionalism of the private security practitioner, in *Seminar of the International Institute for Security and Safety Management*, India.
- Posthumus, S. & Von Solms, R. (2004). A framework for the governance of information security, *Computers & Security*, 23(8): 638-646.
- Pratt, M.K. (2006). *Employee Security Training: Beyond Posters*, Accessed on 12/05/2006. Available at: <http://www.computerworld.com/printthis/2006/0,4814,110494,00.html>.
- PriceWaterhouseCoopers (2004). *Information Security Breaches survey*, Accessed 30/05/2005. Available at: <http://www.pwc.com/extweb/pwcpublishings.nsf/docid/7FA80D2B30A116D7802570B9005C3D16>.
- PriceWaterhouseCoopers & Dti (2005). *Information Security Breaches Survey 2006*, Accessed on 13/12/2005. Available at: [www.security-survey.gov.uk](http://www.security-survey.gov.uk).
- Raikow, D. (2000). *Disclosure Revisited*, Accessed on 16/06/2005. Available at: <http://www.exite.com/news>.
- Rash, W. (2004). *Culture shock*, Accessed on 13/04/2005. Available at: <http://www.infoworld.com>.
- Reim, A. (2000). Cybercrime of the 21st century, *Computer Fraud & Security*, 2001(3): 13-15.
- Roberts, P. (2004). *Sasser a warning of things to come*, Accessed on 15/02/2005. Available at: [http://www.infoworld.com/article/04/05/07/19NNsasser\\_1.html](http://www.infoworld.com/article/04/05/07/19NNsasser_1.html).
- Rossouw, D. (2002). *Part 1&2: Ethical Aspects of IT*, Johannesburg, South Africa.
- Rostern, J. (2005). Dangerous Devices, *The Internal Auditor*, 62(5): 29-32.
- Saint-Germain, R. (2005). Information Security Management Best Practice Based ISO/IEC 17799, *Information Management Journal*, 39(4): 60-66.



- SysAdmin, Audit, Network, Security) Institute. (2006), Accessed on 05/09/2006. Available at <http://www.sans.org/about/sans.php>.
- Schou, C.D. (2001). Information Security: International Curriculum Projects, in *Proceedings of the IFIP WG 11.8 Second World Conference on Information Security Education*, Perth, Australia.
- Schultz, E. (2004). Security training and awareness-fitting a square peg in around hole, *Computers & Security*, 23(1): 1-2.
- Seifried, K. (2000). *Ethics in Information Security*, Accessed on 07/06/2005. Available at: [http://www.seifried.org/security/index.php/Closet20000531\\_Ethics\\_in\\_Information\\_Security](http://www.seifried.org/security/index.php/Closet20000531_Ethics_in_Information_Security)
- Sullivan, B. (2002). *Release of organ donor data prompts changes*, Accessed on 13/02/2005. Available at: <http://archives.cnn.com/2002/TECH/internet/02/16/organ.donor.data.idg/>.
- Sullivan, B. (2005). *Deloitte predicts the future of technology*, Accessed on 02/02/2006. Available at: [www.infoworld.com](http://www.infoworld.com).
- Siponen, M.T. (2000a). A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, 8(1): 31-41.
- Siponen, M.T. (2000b). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice, *Information Management & Computer Security*, 8(5): 197-209.
- Siponen, M.T. (2001). Five Dimensions of Information Security Awareness, *Computers and Society*, 31(2): 24-29.
- Slay, J. & Lock, P. (2005). Developing an undergraduate IT security stream: industry certification and the development of graduate qualities, in *Proceedings of WISE4*, Moscow, Russia, pp. 57-66.
- Smith, E. (2000). *Information Security in Health-Care Systems: a New approach to IT Risk Management*, PhD Degree. Rand Afrikaans University.
- Smith, E., Kritzing, E., Oosthuizen, H.J. & Von Solms, S.H. (2004). Information Security Education, in *Proceedings of the WISE 4 Conference*, Moscow, Russia.
- South African Government (2002). Electronic Communications and Transactions Act [No. 25 of 2002], *Government Gazette*, 446(23708).
- Spurling, P. (1995). Promoting security awareness and commitment, *Information Management & Computer Security*, 3(2): 20-26.

- Squara, D. (2000). *LAN security will become a priority in the networks of tomorrow*, Accessed on 13/02/2005. Available at:  
<http://www.itweb.co.za/sections/techforum/2000/0006290814.asp?A=TEC&S=TechForum&T=Editorial&O=L>
- Streff, K. & Zhou, Z. (2006). Developing and enhancing a computer and network security curriculum, *Journal of Computing Sciences in Colleges*, 21(3): 4-18.
- The White House (2000). *Defending America's Cyberspace: National Plan for Information Systems Protection*, Accessed on 14/07/2005. Available at:  
[www.fas.org/irp/offdocs/pdd/CIP-plan.pdf](http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf).
- Thomson, K. & Von Solms, R. (2005). Information Security obedience: a definition, *Computers & Security*, 24(1): 69-75.
- Thomson, M. (1999). Make information security awareness and training more effective, in *Proceedings of the IFIP, TC 11.8 First World Conference on Information Security Education*, Kista, Sweden.
- Thomson, M.E. & Von Solms, R. (1998). Information security awareness: educating your users effectively, *Information Management & Computer Security*, 6(4): 167-173.
- Turnbull, S. (2003). Network governance, *Corporate Governance International*, 6(3): 4-14.
- Vaughn, R.B., Dampier, D.A. & Warkentin, M.B. (2004). Building an information security education program, in *Proceedings of the 1st annual conference on Information security curriculum development*, pp. 41-45. ACM Press, Kennesaw, Georgia.
- Verine, E. (2004). *Legal implications of information security governance. LLM degree*, Rand Afrikaans University.
- Vinten, G. (1998). Corporate governance: an international state of the art, *Managerial Auditing Journal*, 13(7): 419-431.
- Vinten, G. (2000). Corporate governance: the need to know, *Industrial and Commercial Training*, 32(5): 173-178.
- Von Solms, R. (1998). Information Security Management (2): Guidelines to the management of information technology security (GMITS), *Information Management & Computer Security*, 6(5): 221-223.
- Von Solms, R. & Von Solms, S.H. (2004a). From policies to culture, *Computers & Security*, 23(4): 275-279.

- Von Solms, R. & Von Solms, S.H. (2004b). The 10 deadly sins of information security management, *Computers & Security*, 23(5): 371-376.
- Von Solms, R. & Von Solms, S.H. (2005). From information security to. business security? *Computers & Security*, 24(4): 271-273.
- Von Solms, S.H. (1999). Information Security Management through Measurement, in *Proceedings of the SEC99 conference*, Johannesburg, South-Africa.
- Von Solms, S.H. (2000). Information Security - The third wave, *Computers & Security*, 19(7): 615-620.
- Von Solms, S.H. (2001a). Information Security - A Multidimensional Discipline, *Computers & Security*, 20(6): 504-508.
- Von Solms, S.H. (2001b). Corporate Governance and Information Security, *Computers & Security*, 20(3): 215-218.
- Von Solms, S.H. (2005a). Information Security governance COBIT or ISO 17799 or both? *Computers & Security*, 24(2): 99-104.
- Von Solms, S.H. (2005b). Information Security Governance in ICT Based Educational Systems, *Proceedings of the 2005 Conference in Bangkok*. 109-119.
- Von Solms, S.H. (2005a). Information Security Governance - Compliance management vs operational management, *Computers & Security*, 24(6): 443-447.
- Von Solms, S.H. & Eloff, J.H.P. (2004). *Information Security*. University of Johannesburg, Johannesburg, South-Africa.
- Wager, R. (2005). *Building Your Information Security Awareness Program*, Accessed on 03/02/2006. Available at: [www.gartner.com](http://www.gartner.com).
- Waint, T.L. (2005). Information security policy's impact on reporting security incidents, *Computers & Security*, 24(6): 448-459.
- Werner, L. (2004). Teaching Principled and practical information, *Journal of Computing Sciences in Colleges*, 20(1): 81-89.
- Whiteman, W. (2004). In defense of the realm: understanding the threats of information Security, *International Journal of Information Management*, 24(1): 43-57.
- Whiteman, W. & Mattord, H.J. (2003). *Principles of Information Security*, Thomson, Canada.
- Williams, J. (2005). *IT Education: More Specialized in 2010*, Accessed on 03/03/2006. Available at: <http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/mags/it/&toc=comp/mags/it/2004/06/f6toc.xml&DOI=10.1109/MITP.2004.86>

- Williams, P. (2001). Information Security Governance, *Information Security Technical Report*, 6(3): 60-70.
- Wills, M. (1999). First c:ure Certificates Presented by Minister, *c:ure world*: 1.
- Wilson, M. & Hash, J. (2005). *Information Technology security awareness, training, education and certification*, Available at:  
<http://www.itl.nist.gov/lab/bulletns/bltnoct03.htm>.
- Wood, C.C. (1995). Information Security Awareness Raising Methods, *Computer Fraud & Security*, June 1995: 13-15.
- Wood, C.C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature, *Computer Fraud & Security*, 2004(1): 16-17.
- Wright, M.A. (1998). The Need for Information Security Education, *Computer Fraud & Security*, 1999(8): 14-17.
- Yang, T.A. (1998). Computer Security and impact on Computer Science Education, *The Journal of Computing in Small Colleges*, 16(4): 233-246.
- Yasubsac, A. (2002). Information Security Curricula in Computer Science Departments: Theory and Practice, *Journal of Information Security*, 1(2).
- Yngstrom, L. & Bjorck, F. (2004). The Value and Assessment of Information Security Education and Training, in *Proceedings of WISE*.
- Yurcik, W. & Doss, D.L. (2001). Different Approaches in the Teaching of Information Systems Security, in *The Proceedings of the ISECON conference*.
- Zhu, K., Xu, S. & Kraemer, K.L. (2006). *Global E-Commerce: Impacts of National Environments and Policy*, Cambridge University Press.

# **Appendix A**

## **Specifications for a prototype for the Information Security Retrieval and Awareness (ISRA) model**

## A.1 Purpose of the prototype

The purpose of the prototype is to illustrate that the Information Security Retrieval and Awareness (ISRA) model can be implemented successfully. The aim of the ISRA model is to enhance Information Security awareness in industry.

## A.2 Database

All information required for the prototype is stored in a database that consists of eleven tables. The purpose of each table, the columns within that table, together with the type of information to be stored in each column, is provided below. The primary key for each table is underlined.

### A.2.1 Document table

The purpose of this table is to store all the relevant information regarding each state-of-the-art Information Security document.

<u>Document ID</u>	Name	Location	Created	CreatedBy	Modified	ModifiedBy
Numeric	Text	Text	Date	Text	Date	Text

- The `DocumentID` column uniquely identifies each Information Security document.
- The `Name` column contains the official name of the document.
- The `Location` column contains information regarding the publication details of the document.
- The `Created` column contains the date on which the document was added.
- The `CreatedBy` column contains the name of the user who added the document.
- The `Modified` column contains the date on which the document was last modified.
- The `ModifiedBy` column contains the name of the user who last modified the document.

### A.2.2 BodyOfKnowledge Table

The purpose of this table is to store all the relevant information within the Body of Knowledge for Information Security of the ISRA model.

<u>BoKID</u>	Content	Created	CreatedBy	Modified	ModifiedBy
Numeric	Text	Date	Text	Date	Text

- The `BoKID` column uniquely identifies each information section within the Body of Knowledge.
- The `Content` column contains the information that will be added to the Body of Knowledge.
- The `Created` column contains the date on which the information was added.
- The `CreatedBy` column contains the name of the user who added the information.
- The `Modified` column contains the date on which the information was last modified.
- The `ModifiedBy` column contains the name of the user who last modified the information.

### A.2.3 Level Table

The purpose of this table is to store all the relevant information regarding IT authority levels that form part of the ISRA model.

<u>LevelID</u>	Name	Details	Created	CreatedBy	Modified	ModifiedBy
Numeric	Text	Text	Date	Text	Date	Text

- The `LevelID` column uniquely identifies each IT authority level.
- The `Name` column contains the official name of the IT authority level.
- The `Details` column contains detailed information regarding each IT authority level.
- The `Created` column contains the date on which the IT authority level was added.
- The `CreatedBy` column contains the name of the user who added the IT authority level.
- The `Modified` column contains the date on which the IT authority level was last modified.
- The `ModifiedBy` column contains the name of the user who last modified the IT authority level.

### A.2.4 Issue Table

The purpose of this table is to store all the relevant information regarding the non-technical Information Security issues that form part of the ISRA model.

<u>IssueID</u>	Name	Details	Created	CreatedBy	Modified	ModifiedBy
Numeric	Text	Text	Date	Text	Date	Text

- The `IssueID` column uniquely identifies each Information Security issue.
- The `Name` column contains the official name of the Information Security issue.
- The `Details` column contains extra information regarding an Information Security issue.
- The `Created` column contains the date on which the Information Security issue was added.
- The `CreatedBy` column contains the name of the user who added the Information Security issue.
- The `Modified` column contains the date on which the Information Security issue was last modified.
- The `ModifiedBy` column contains the name of the user who last modified the Information Security issue.

### A.2.5 Detail Table

The purpose of this table is to connect the `Document`, `Issue` and `Level` tables to the `Body of Knowledge` table in order to establish who should be aware of what information.

<u>DetailID</u>	DocumentID	Issue ID	LevelID	BoKID
Numeric	Numeric	Numeric	Numeric	Numeric

- The `DetailID` column is a unique identifier.
- The `DocumentID` column uniquely identifies each Information Security document.
- The `IssueID` uniquely identifies each Information Security issue.
- The `LevelID` uniquely identifies each IT authority level.
- The `BoKID` uniquely identifies each section of information within the `Body of Knowledge`.



### A.2.6 Employee Table

The purpose of this table is to store all the relevant information regarding all the employees within the organisation.

<u>Employee ID</u>	Level ID	First-Name	Sur-name	User-name	Pass-word	Created	Created-By	Modified	Modified-By
Numeric	Text	Date	Text		Text	Date	Text	Date	Text

- The `EmployeeID` column uniquely identifies each employee.
- The `LevelID` column identifies the IT authority level of that employee.
- The `FirstName` column contains the official first name of the employee.
- The `Surname` column contains the official surname of the employee.
- The `Username` column contains the username of each employee.
- The `Password` column contains the employee's password in encrypted format.
- The `Created` column contains the date on which the employee was added.
- The `CreatedBy` column contains the name of the user who added the employee.
- The `Modified` column contains the date on which the information about the employee was last modified.
- The `ModifiedBy` column contains the name of the user who last modified the information about the employee.

### A.2.7 Statistic Table

The purpose of this table is to store all the statistical results generated by the prototype.

<u>Statistic</u>	Employee ID	IssueID	TestMark	Created	Created-By	Modified	Modified-By
Numeric	Text	Numeric	Numeric	Date	Text	Date	Text

- The `Statistic` column uniquely identifies each test mark for each employee and Information Security issue.
- The `EmployeeID` column identifies the specific employee.
- The `IssueID` column identifies the specific Information Security issue.
- The `TestMark` column identifies the latest test result.
- The `Created` column contains the date on which the statistic was created.
- The `CreatedBy` column contains the name of the user who created the statistic.
- The `Modified` column contains the date on which the statistic was last modified.

- The `ModifiedBy` column contains the name of the user who last modified the statistic.

### A.2.8 Question Table

The purpose of this table is to store all the questions needed for the Information Security awareness tests.

<u>QuestionID</u>	Question	Created	CreatedBy	Modified	ModifiedBy
Numeric	Text	Date	Text	Date	Text

- The `QuestionID` column uniquely identifies each question.
- The `Question` column identifies the question.
- The `Created` column contains the date on which the question was added.
- The `CreatedBy` column contains the name of the user who added the question.
- The `Modified` column contains the date on which the question was last modified.
- The `ModifiedBy` column contains the name of the user who last modified the question.

### A.2.9 Answer Table

The purpose of this table is to store all the answers of the questions needed for the Information Security awareness tests.

<u>AnswerID</u>	Answer	QuestionID	CorrectAnswer	Created	CreatedBy	Modified	ModifiedBy
Numeric	Text	Numeric	Text	Date	Text	Date	Text

- The `AnswerID` column uniquely identifies each answer.
- The `Answer` column contains the answers for questions in the Information Security Awareness tests.
- The `QuestionID` column identifies the appropriate question.
- The `CorrectAnswer` column contains if the answer is correct or not.
- The `Created` column contains the date on which the answer was added.
- The `CreatedBy` column contains the name of the user who added the answer.
- The `Modified` column contains the date on which the answer was last modified.
- The `ModifiedBy` column contains the name of the user who last modified the answer.

### A.2.10 QuestionDetails Table

The purpose of this table is to link the Level and Issue table to a specific question.

<u>QuestionDetailID</u>	LevelID	IssueID	QuestionID
Numeric	Numeric	Numeric	Numeric


- The QuestionDetailID column uniquely identifies a combination of a question, an Information Security issue and an IT authority level.
- The LevelID column identifies the IT authority level.
- The IssueID column identifies the specific Information Security issue.
- The QuestionID column identifies the specific question.

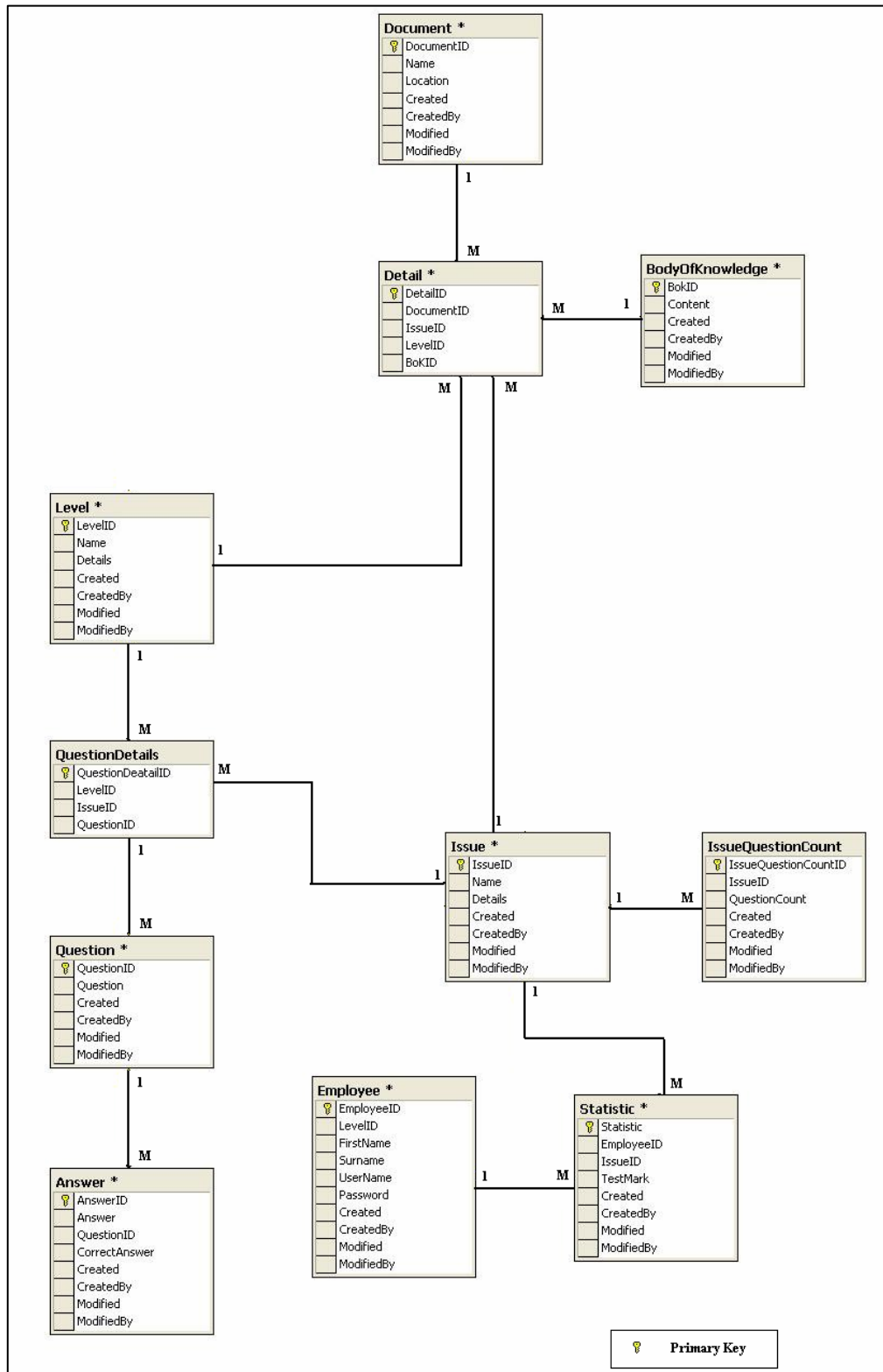
### A.2.11 IssueQuestionCount Table

The purpose of this table is to store the number of questions that will be included in each Information Security awareness test.

<u>IssueQuestionCountID</u>	IssueID	QuestionCount	Created	Created - By	Modified	Modified - By
Numeric	Numeric	Numeric	Date	Text	Date	Text

- The IssueQuestionCountID column contains the unique identifier of this table.
- The IssueID column identifies the Information Security issue.
- The QuestionCount column identifies the number of questions for each Information Security issue.
- The Created column contains the date on which the IssueQuestionCountID was added.
- The CreatedBy column contains the name of the user who added the IssueQuestionCountIID.
- The Modified column contains the date on which the IssueQuestionCountID was last modified.
- The ModifiedBy column contains the name of the user who last modified the IssueQuestionCountID.

The Entity Relationship (E-R) diagram of the database is depicted Figure A1. The primary keys  of each table and the relationships (1:M) between the tables are indicated.



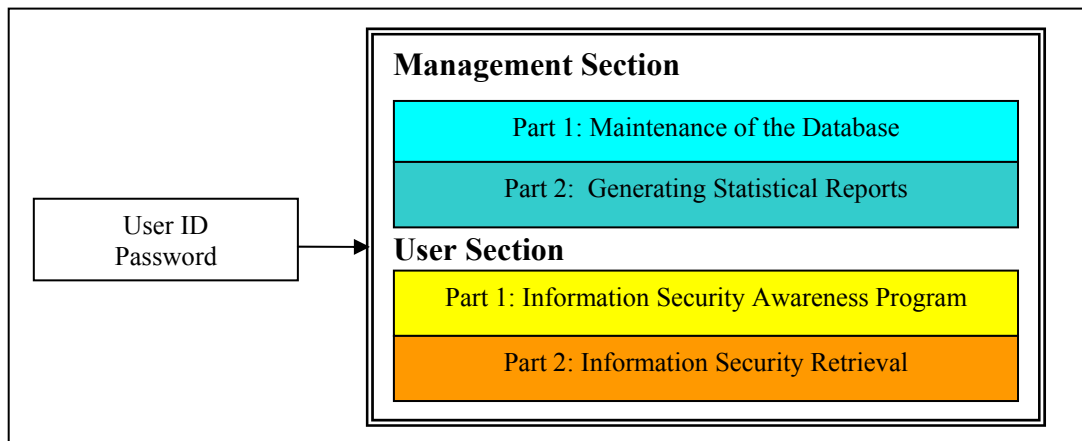
**Figure A1: Entity Relationship Diagram of the ISRA database**

### A.3 Sections of the prototype

The prototype should comprise of two main sections:

- The Management section
- The User section

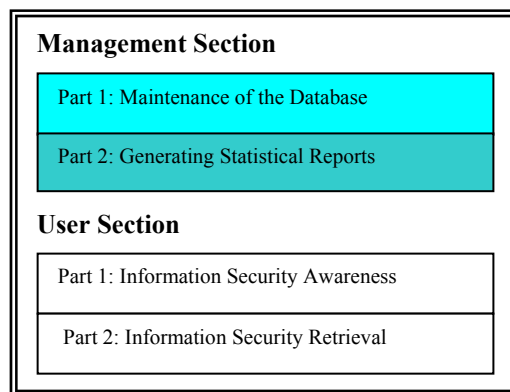
Access to both of these sections should be controlled by means of User ID and password combinations. Each of these two sections is divided further into two parts, as depicted in Figure A2.



*Figure A2: The Management and User Sections*

#### A.3.1 The Management Section

The Management section consists of two parts (i.e. Maintenance of the Database and Generating Statistical Reports) as depicted in Figure A3.



*Figure A3: The Management Section*

The **Information Security Manager** should have access to both parts. He/She should however also have the option of granting any of the other IT authority levels (such as the Board level) access to the second part (i.e. Generating Statistical Reports).

Each of these parts will be discussed in detail in paragraphs A.3.1.1 and A.3.1.2.

### **A.3.1.1 Maintenance of the database**

This part may only be accessed by the Information Security Manager. The purpose of this part is to *add*, *edit* and *delete* information in the database. The Information Security Manager should be able to add, edit or delete information from/to the following tables:

- Body of Knowledge Table
- Document Table
- Employee Table
- Issue Table
- Level Table
- Question Table
- Answer Table

In addition, the Information Security Manager should be able to change the text display on the home page, as well as change the number of questions in the Information Security awareness test related to each Information Security issue.

### **A.3.1.2 Generating Statistical Reports**

The Information Security Manager should by default have access to Part 2 – the generating of statistical reports. He/She should also be able to grant or revoke access to this functionality to any of the IT authority levels in the organisation.

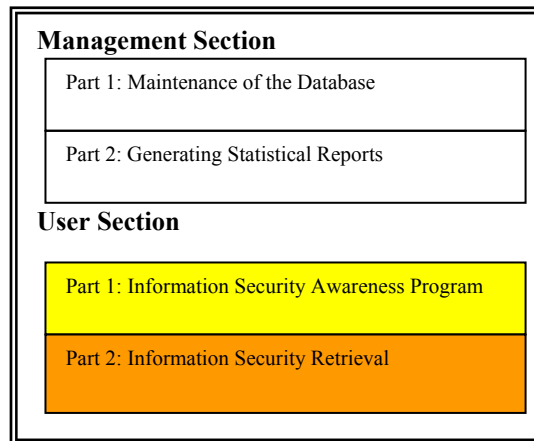
Statistical reports may be requested on an ad hoc basis by an IT authority level (such as the Board level) to determine if the organisation's Information Security awareness status is at an acceptable level and where problem areas lie.

The prototype should generate a report that indicates the status (i.e. test results) of each stakeholder within an IT authority level for each Information Security issue. The user should be able to specify a specific IT authority level and one or more Information Security issues. The reports should present the results both in a tabular format and as a

bar chart. The results should indicate in red which stakeholders are a possible Information Security risk. The rest of the stakeholders should be indicated in green.

### A.3.2 The User Section

The User section contains two parts (i.e. Information Security Awareness Program and the Information Security Retrieval) as depicted in Figure A4.



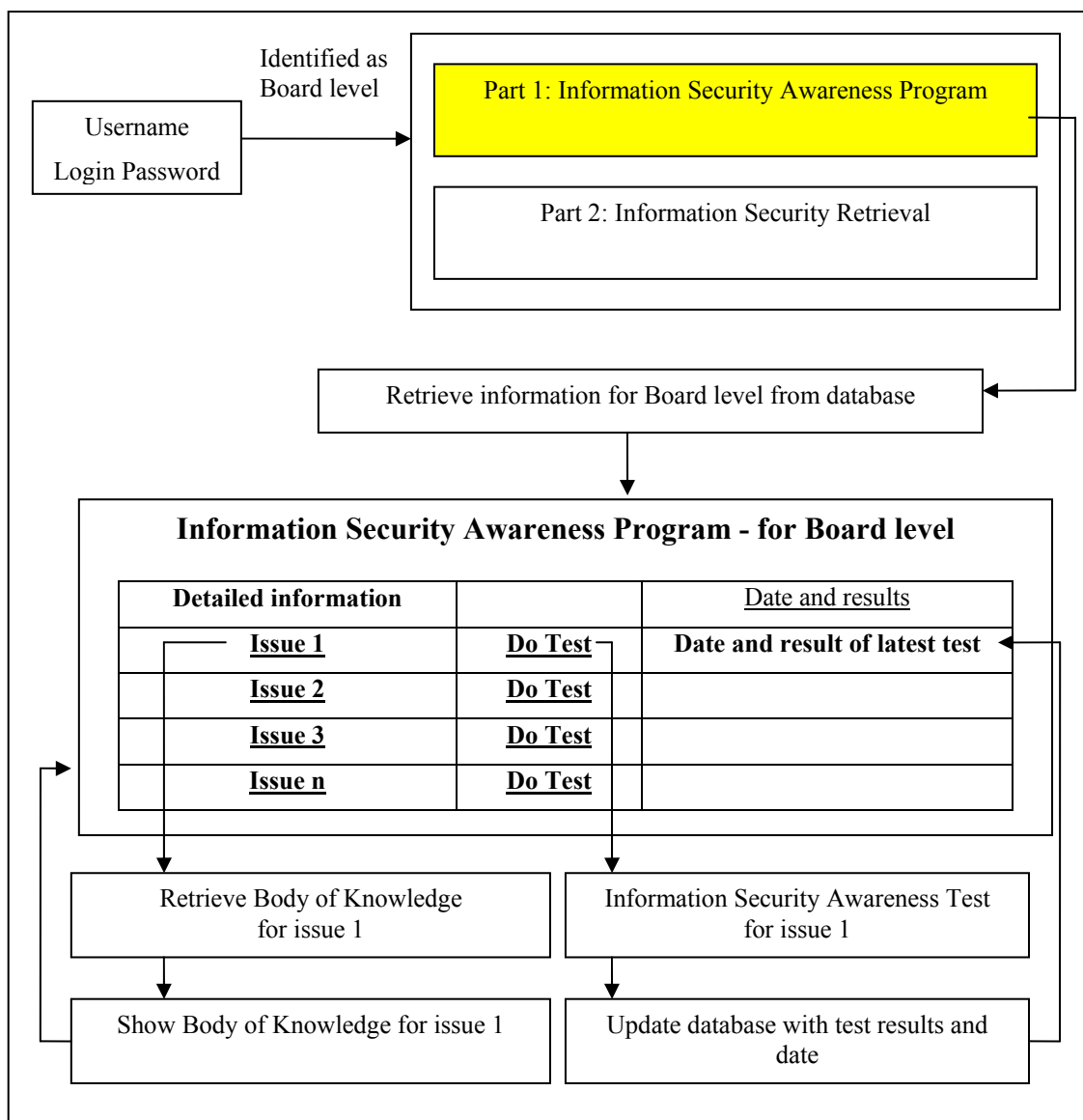
*Figure A4: The User section*

All stakeholders should have access to both parts. These two parts will be discussed in detail in the rest of this paragraph.

#### A.3.2.1 Information Security Awareness Program

The purpose of the Information Security Awareness Program is to measure the status of Information Security awareness among IT authority levels as well as among individual stakeholders in an organisation.

Each IT authority level should have its own Information Security Awareness section that displays only the Information Security issues relevant to that specific IT authority level. The login process should identify the stakeholder's IT authority level and accordingly display the relevant Information Security issues. Consider Figure A5.



**Figure A5: Flow diagram for Information Security Awareness Program**

The example in Figure A5 depicts the logical flow of information when a stakeholder who forms part of the Board level logs in. The prototype identifies the stakeholder as being on the Board level and retrieves the information relevant to the Board level from the database. This information should be displayed in a table format as depicted in Figure A5.

Each Information Security issue should have a link to a separate area where information regarding that Information Security issue can be displayed. Each Information Security issue should also have a link to an Information Security awareness test. This test should consist of multiple choice questions that were set by the Information Security Manager.



The multiple choice questions should be selected from the database randomly every time the test is done. The marks for the latest test completed should be stored in the database and displayed to the stakeholder with the date on which it was completed.

### **A.3.2.2 Information Security Retrieval**

The purpose of the Information Security Retrieval section is to allow stakeholders to become familiar with relevant Information Security issues at their own time and at their own pace. This is achieved by providing stakeholders with various options for retrieving and studying information regarding Information Security issues, without the need to involve another person.

A stakeholder should be able to choose the following options:

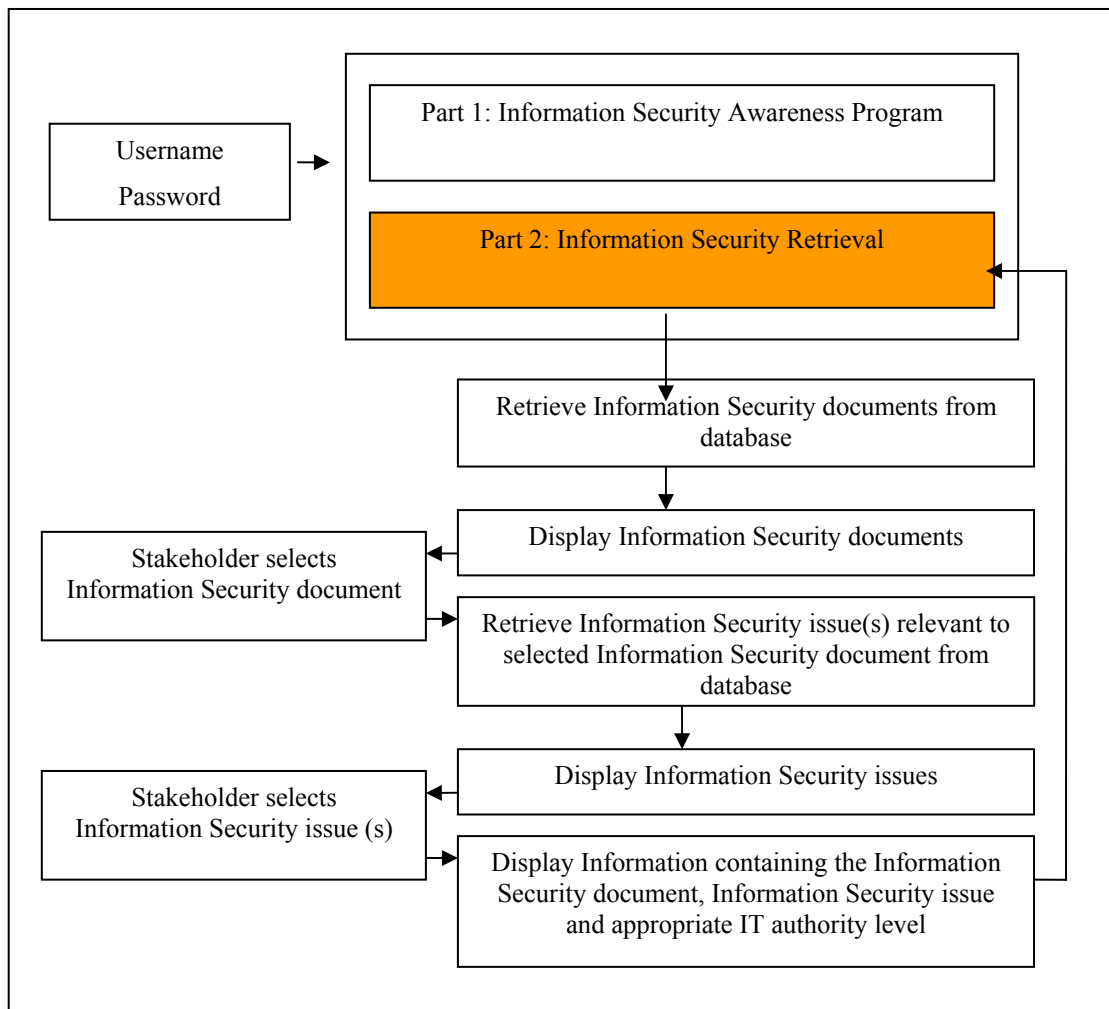
- Information on Information Security Documentation (A.3.2.2.1)
- Information on Information Security Issues (A.3.2.2.2)

The information retrieved in this part will be used to enhance Information Security awareness among all IT authority levels, as well as to assist persons on different IT authority levels with decision-making processes.

#### **A.3.2.2.1 Information Security Documentation**

The purpose of this option is to retrieve relevant information regarding different Information Security documents. In this option the Information Security document is the primary source.

See Figure A6.



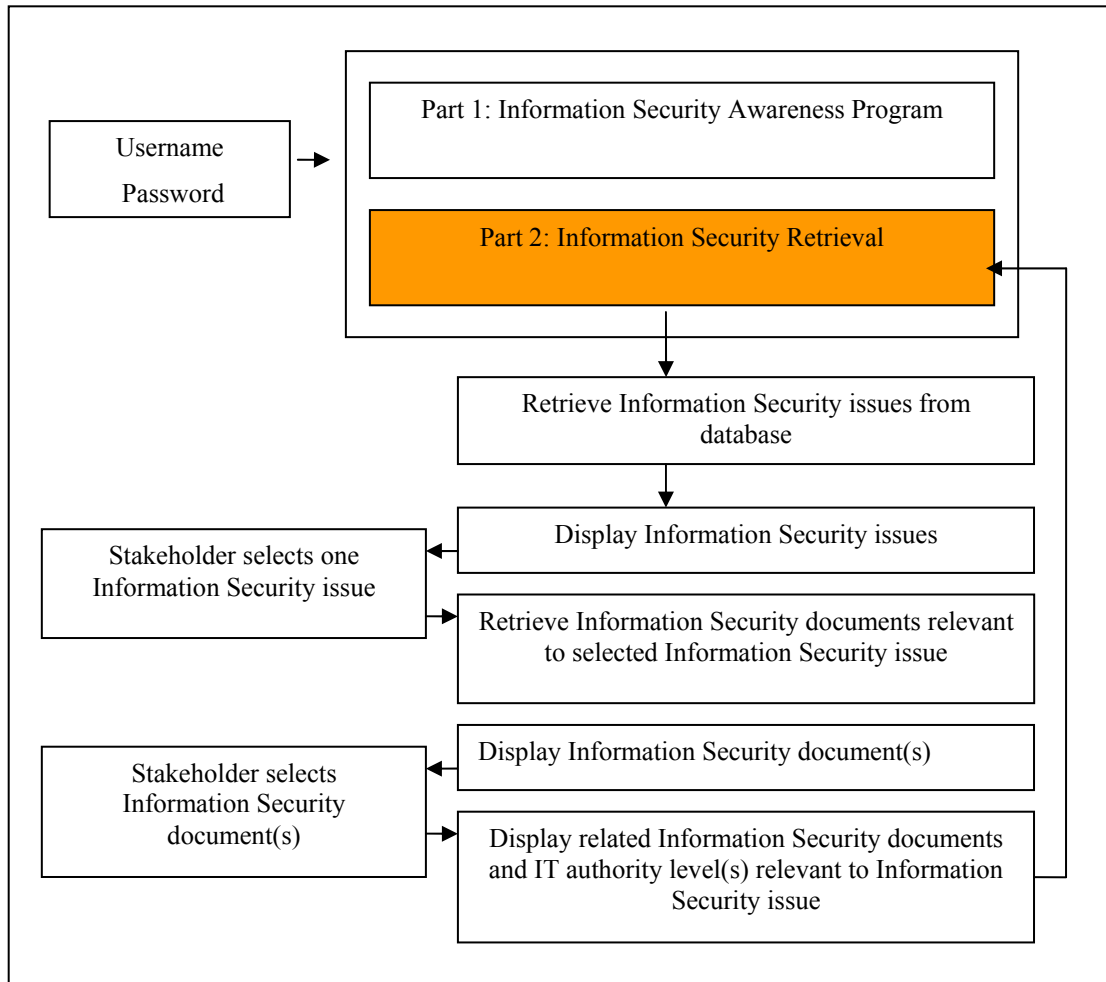
**Figure A6: Retrieval of Information Security documents**

The stakeholder should be able to select **one** Information Security document at a time so as to obtain detailed information on it. After the stakeholder has selected the Information Security document, the relevant Information Security issues for that document should be displayed. The stakeholder should then be able to select **one or more** of these Information Security issues.

The following information should be displayed as a result: Information contained in the selected Information Security document regarding the Information Security issue(s) selected, as well as those IT authority levels that should be aware of these issues according to the current Information Security document.

### A.3.2.2.2 Information on Information Security Issues

The purpose of this option is to retrieve relevant information regarding different Information Security issues. In this option the Information Security issues are the primary source. See Figure A7.



**Figure A7: Retrieval of Information Security issues**

The stakeholder should be able to select **one** Information Security issue on which to obtain detailed information. After he/she has selected the Information Security issue, the relevant Information Security documents for that issue should be displayed. The stakeholder should then be able to select **one or more** of the Information Security documents.

The following should be displayed as a result: Information regarding the selected Information Security issues as contained in each Information Security document selected,

as well as those IT authority levels that should be aware of this issue, based on each document selected.

# **Appendix B**

## **Prototype user's guide**

## **B.1 Getting Started**

### **B.1.1 Technical Details**

The prototype was developed by IT-Event Management and can be found at the following URL: <http://www.it-em.co.za/isra>. This website was developed in Microsoft Visual Studio .Net 2003 using Visual Basic and JavaScript. The server hosting this website needs to have the .Net Framework SDK v1.1 installed and a valid Cute Soft, cute editor licence (<http://www.cutesoft.net/>). SQL Server 2000 service pack 3 is used for the database and the server is running Windows 2003 server service pack 1. The site is best viewed using Internet Explorer 6.

### **B.1.2 Conventions used**

The prototype user's guide employs the following conventions:

- Typeface "Courier New" is used to present text as it appears on the screen.
- Typeface "Arial" is used to present an action by the user.

### **B.1.3 Instructions for executing the prototype**

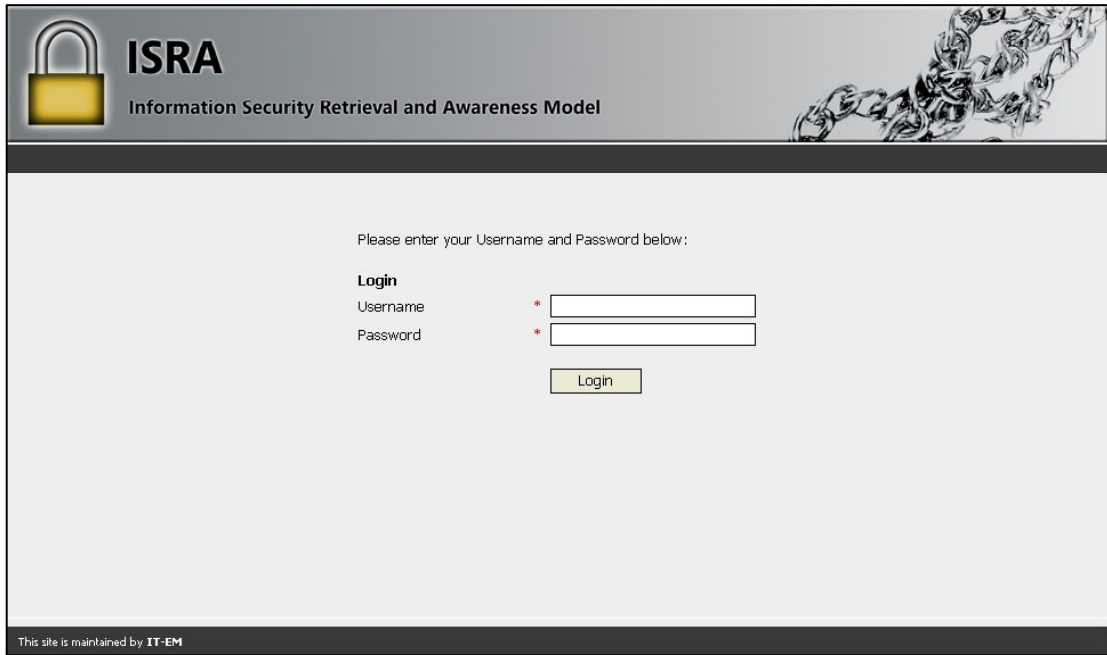
The prototype can be found at the following URL: <http://www.it-em.co.za/isra>.

<p><b>Note that the execution of the application will improve dramatically when executed in an Intra-net environment that adheres to all the software specifications as detailed in paragraph B.1.1</b></p>
---

## **B.2 Working with the Prototype**

### **B.2.1 Login process**

When the prototype is loaded, it presents you with the login screen depicted in Figure B1.



**Figure B1: Login screen**

The Login is the first step in the process of using the prototype. All users of the system will be provided with a Username and Password by the Information Security Manager. All passwords are saved in an encrypted format in the database to enhance the security of the system. In the Login process it is compulsory that you provide both your Username and Password (indicated with black dots) to obtain access to the system. For the purpose of testing the prototype, enter “elmarie” for the username and “password” for the password.

If you click on the Login button (depicted in Figure B1) *without* providing your Username and password, the error message (depicted in Figure B2) will be displayed. To proceed, click on the OK button and enter your Username and password.



**Figure B2: Incorrect username and password**

If you click on the `Login` button without providing either your username or your password, Figure B3 or B4 will be displayed. To proceed, click on the `OK` button and enter required information.

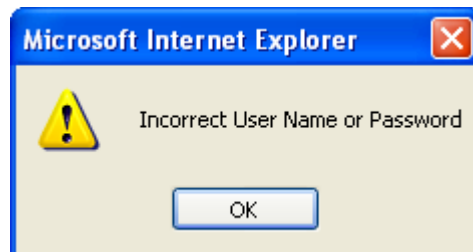


***Figure B3: Username required***



***Figure B4: Password required***

If you provide either an incorrect Username or an *incorrect* Password, the system will display an error message (depicted in Figure B5) informing you that an incorrect Username or an incorrect Password has been supplied.

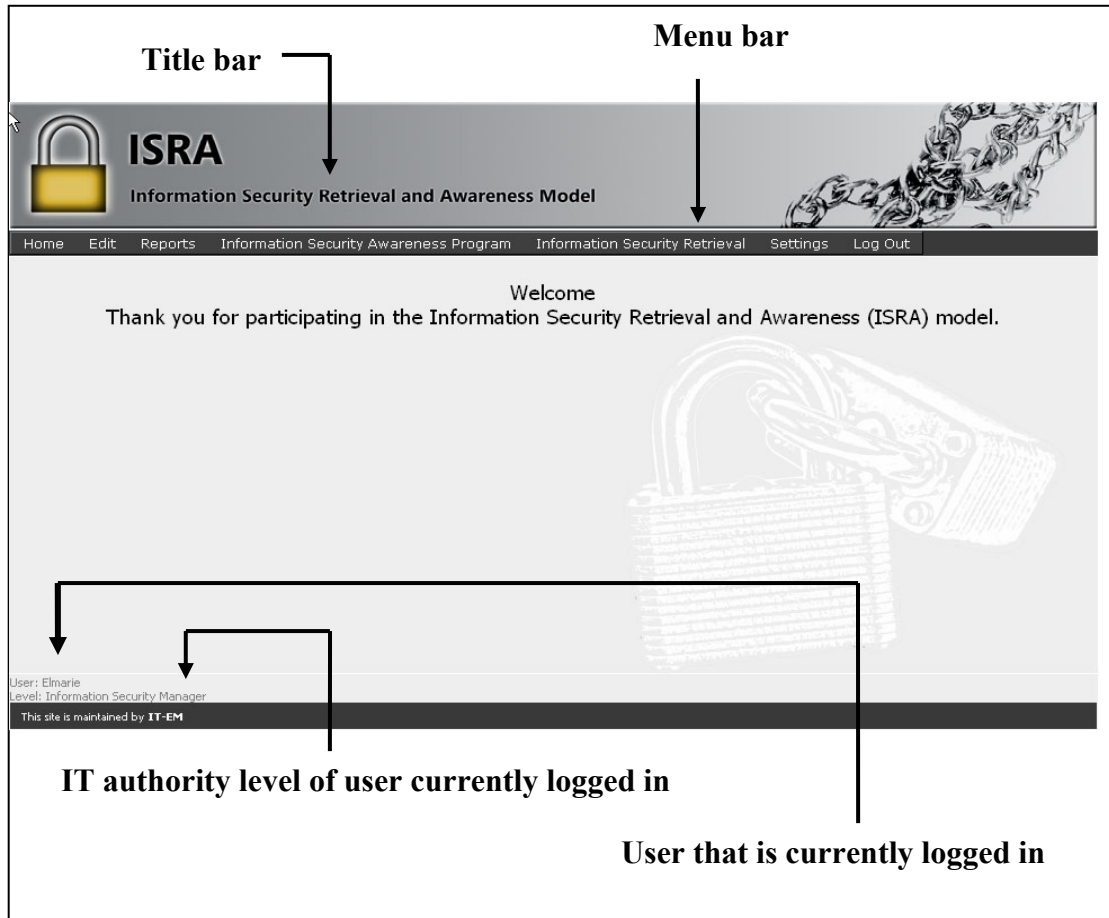


***Figure B5: Incorrect Username or Password***

To proceed, click on the `OK` button and re-enter your Username or Password. The Home screen will be displayed as depicted in Figure B6.



## B.2.2 Home Page



*Figure B6: Home page*

At the top of the Home screen a Title and a Menu bar is depicted. The different options (Home, Edit, Reports, Information Security Awareness Program, Information Security Retrieval, Settings and Log Out) on the Menu bar will each be discussed in detail. At the bottom of the Home screen the Username and the IT authority level of the current user are indicated. To return to this page at any time, select the Home option on the menu bar.

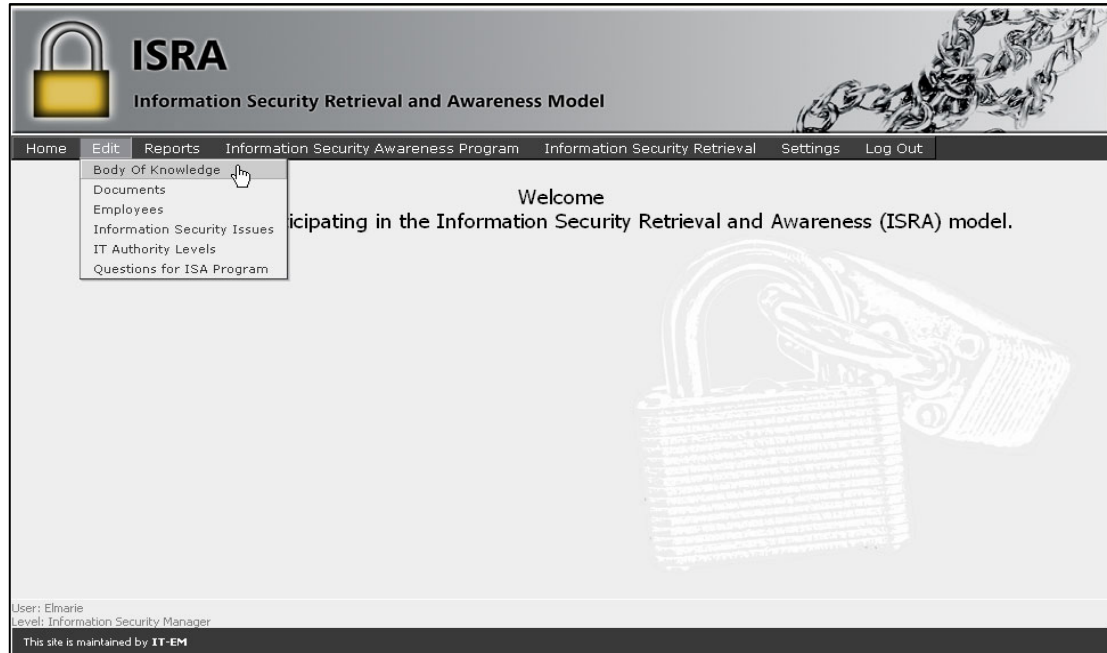
## B.2.3 Edit function

The Edit function includes the following sub menu options: Body of Knowledge (B.2.3.1), Documents (B.2.3.2), Employees (B.2.3.3), Information Security Issues (B.2.3.4), IT Authority Levels (B.2.3.5), Questions for ISA

Program (B.2.3.6). Each of these sub menu options will be discussed in detail in the rest of this paragraph.

### B.2.3.1 Body of Knowledge

If you want to edit the Body of Knowledge, click on the Body of Knowledge option under the Edit menu option as depicted in Figure B7.



*Figure B7: Edit the Body of Knowledge*

After you have clicked on the Body of Knowledge option, the current Body of Knowledge for Information Security is displayed as depicted in Figure B8.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Notes:**

- Click on content to view/ update or delete the content related to a specific Information Security Issue
- Click on the Add button to add to the Body of Knowledge

Add

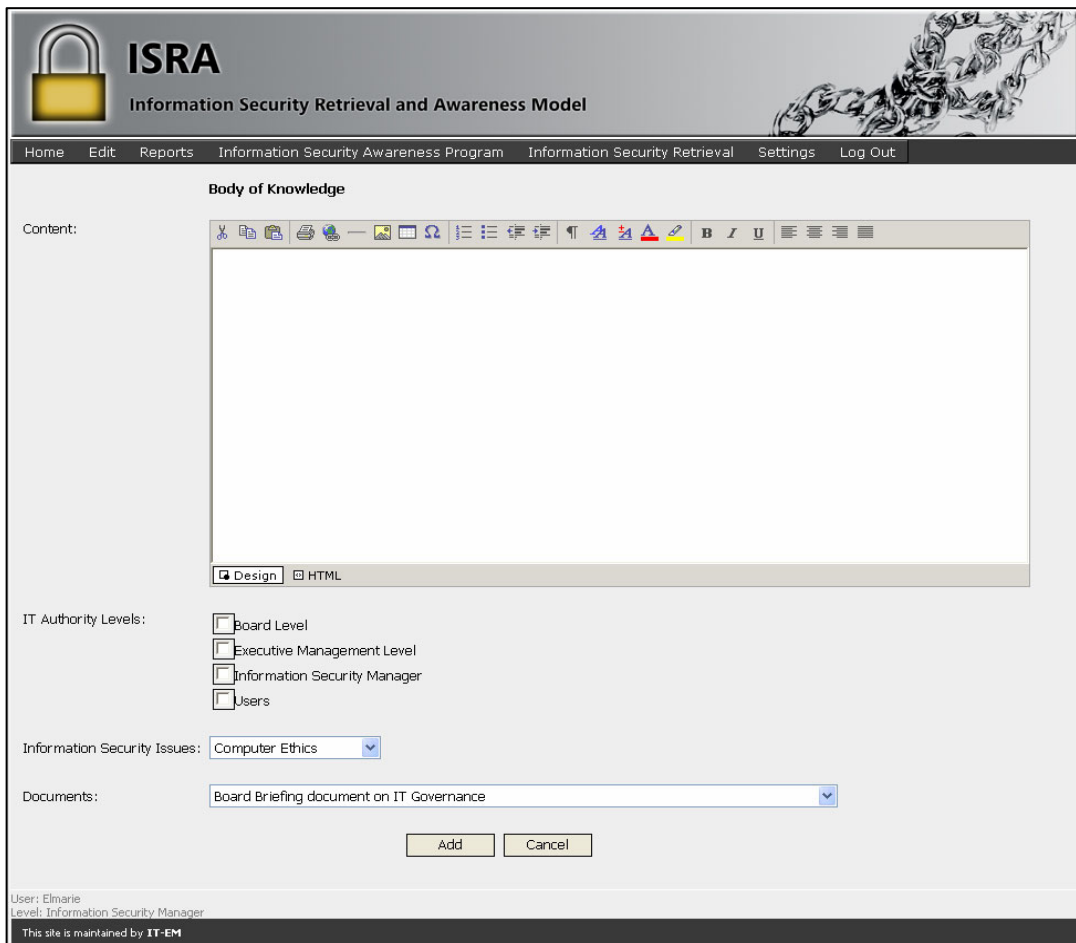
< Prev 10 Next 10 >

Content	Information Security Issue	Document
According to NIST senior management has ultimate r...	Corporate Governance	National Institute of Standards (NIST) handbook
For Information Security to be properly addressed,...	Corporate Governance	Information Security Governance: Guidance for Boards of Directors and Executive Management
Physical and environmental security controls are i...	Physical Security	National Institute of Standards (NIST) handbook
The senior management needs to have considered the...	Security Policy	Commonwealth Protective Security Manual
A policy document should be approved by management...	Security Policy	International Organization for Standardization Standard 17799 (ISO 17799)
Corporate Governance is to: Setting aims P...	Corporate Governance	Board Briefing document on IT Governance
Effective communication of its strategic plans and...	Corporate Governance	The KING report
Empowered to support the enterprise's ethical prin...	Computer Ethics	The KING report
Establish the values of the enterprise in support...	Computer Ethics	The KING report
Agency employees, contractors and contractor emplo...	Physical Security	Commonwealth Protective Security Manual

< Prev 10 Next 10 >

**Figure B8: Current Body of Knowledge for Information Security**

To add information to the Body of Knowledge, click on the Add button (as depicted in Figure B8). You will then be presented with the screen depicted in Figure B9.



**Figure B9: Add to the Body of Knowledge**

To add the new information, type it in the `Content` box. Thereafter, select the IT authority levels to whom this information is relevant. Click on the check box next to each IT authority level that needs to be aware of this information. A tick mark will appear in the box when you click. To remove such a tick mark, just click on it and it will disappear. The next step is to select the Information Security issue that forms part of this new information. Click on the arrow of the dropdown list next to `Information Security Issues` and click on the relevant issue. Note that only one issue can be selected. Click on the arrow of the dropdown list next to `Documents` and click on the relevant Information Security document. Finally, you need to specify the origin of this information. Alternatively, if you are sure that all information entered is correct and complete, click on the `Add` button to add the information to the Common Body of Knowledge.

The database will now be updated to include this new information, and the initial screen (Figure B8) will be displayed again. To view the new information added, click on the Next 10 link in the top or bottom row of the table (depicted in B8) until the new information is displayed. The new information is displayed in the last row of the table as depicted in Figure B10.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Notes:**

- Click on content to view/ update or delete the content related to a specific Information Security Issue
- Click on the Add button to add to the Body of Knowledge

Add

< Prev 10 Next 10 >

Content	Information Security Issue	Document
<a href="#">An Information Security Policy is important...</a>	Security Policy	The KING report
<a href="#">Management should create a framework and an awar...</a>	Computer Ethics	Governance, Control and Audit for Information and Related Technology (COBIT)
<a href="#">All employees should be aware of all policies&amp;nb...</a>	Security Policy	International Organization for Standardization Standard 17799 (ISO 17799)
<a href="#">All personnel should be trained and educated in...</a>	Computer Ethics	Board Briefing document on IT Governance
<a href="#">Senior management is responsible for developing an...</a>	Security Policy	Governance, Control and Audit for Information and Related Technology (COBIT)
<a href="#">The security policy serves as the basis for establ...</a>	Security Policy	National Institute of Standards (NIST) handbook
<a href="#">An Information Security Policy is important...</a>	Security Policy	The KING report
<a href="#">Ultimately, responsibly for the success of an orga...</a>	Security Policy	National Institute of Standards (NIST) handbook
<a href="#">The agency head is responsible for ensuring that t...</a>	Corporate Governance	Financial Aspects of Corporate Governance report (Cadbury report)
<a href="#">The agency head is responsible for ensuring that t...</a>	Computer Ethics	Commonwealth Protective Security Manual

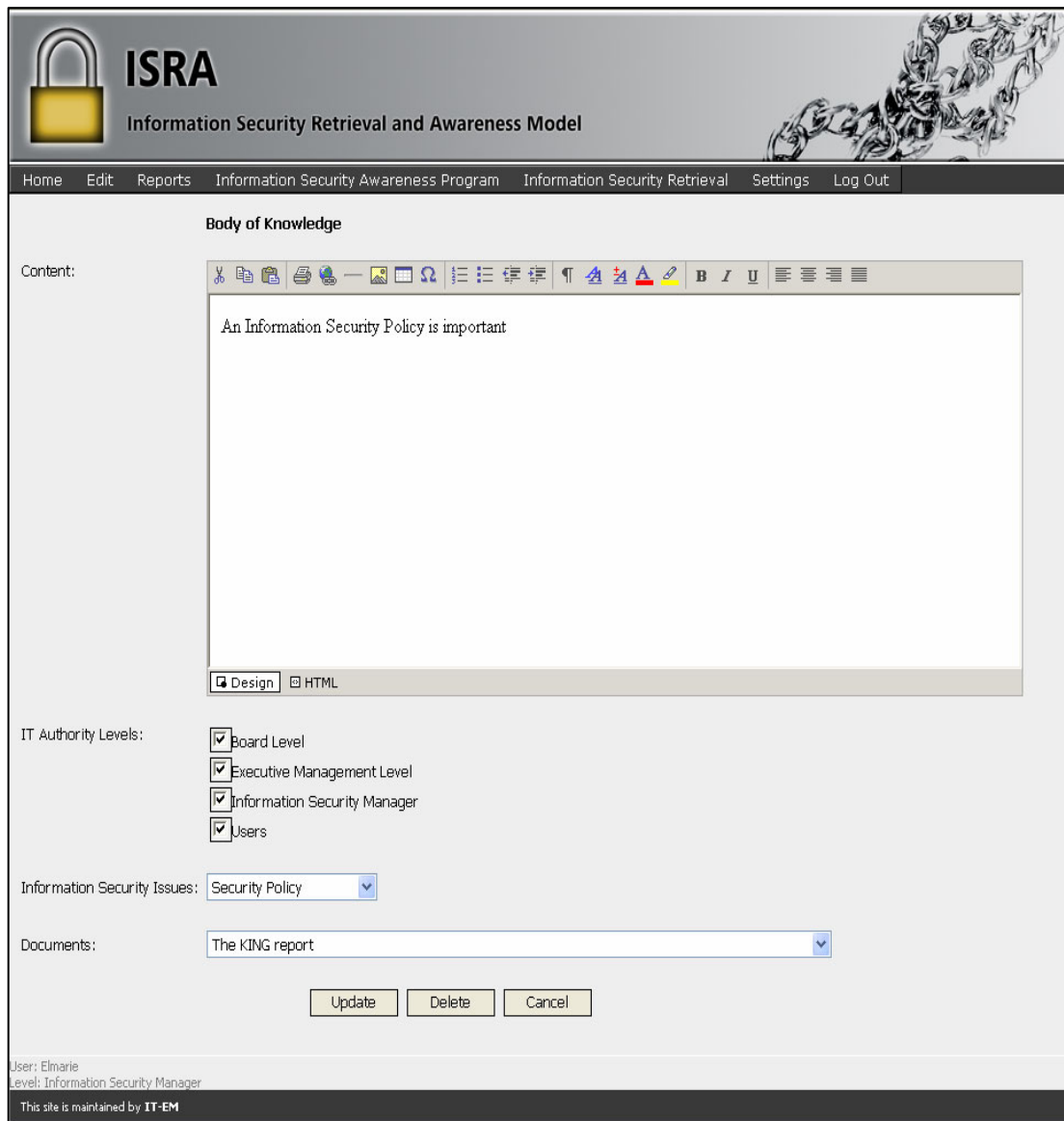
< Prev 10 Next 10 >

User: Elmarie  
Level: Information Security Manager  
This site is maintained by IT-EM

**Figure B10: Select information to be deleted or updated**

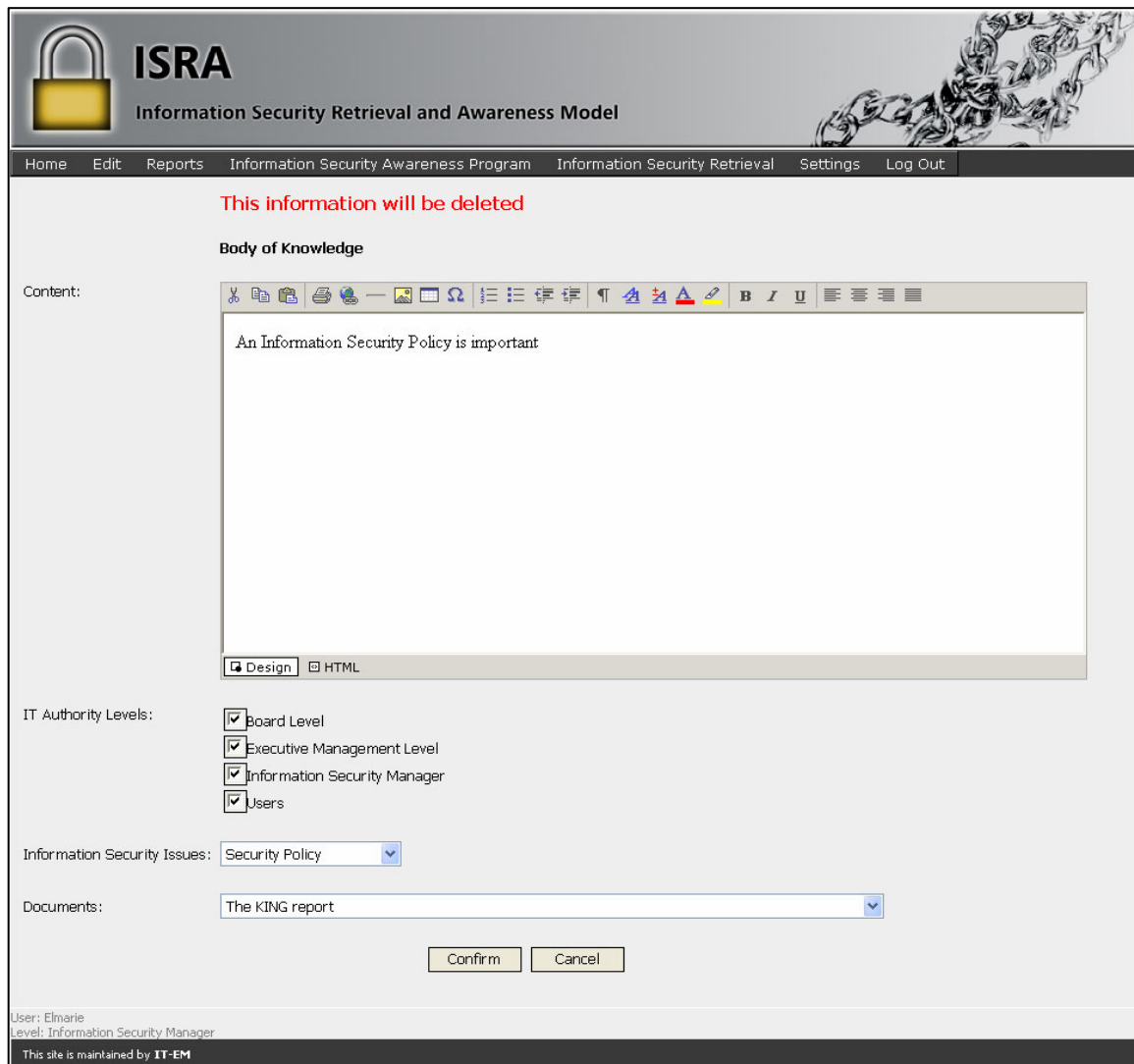
To edit (update or delete) information for the Body of Knowledge, click on the information displayed in the Content column that you want to edit as indicated in Figure B10.

You will accordingly be presented with Figure B11.



**Figure B11: Update or delete information from the Body of Knowledge**

You can either update or delete the selected information. If you want to return to the initial screen without deleting the information, click on the `Cancel` button. Alternatively, if you want to update the Common Body of Knowledge, make the necessary changes and click on the `Update` button at the bottom of the screen. If you want to delete the document, click on the `Delete` button at the bottom of the screen. The system will prompt you to confirm the `Delete` action. See Figure B12 – top of the screen.

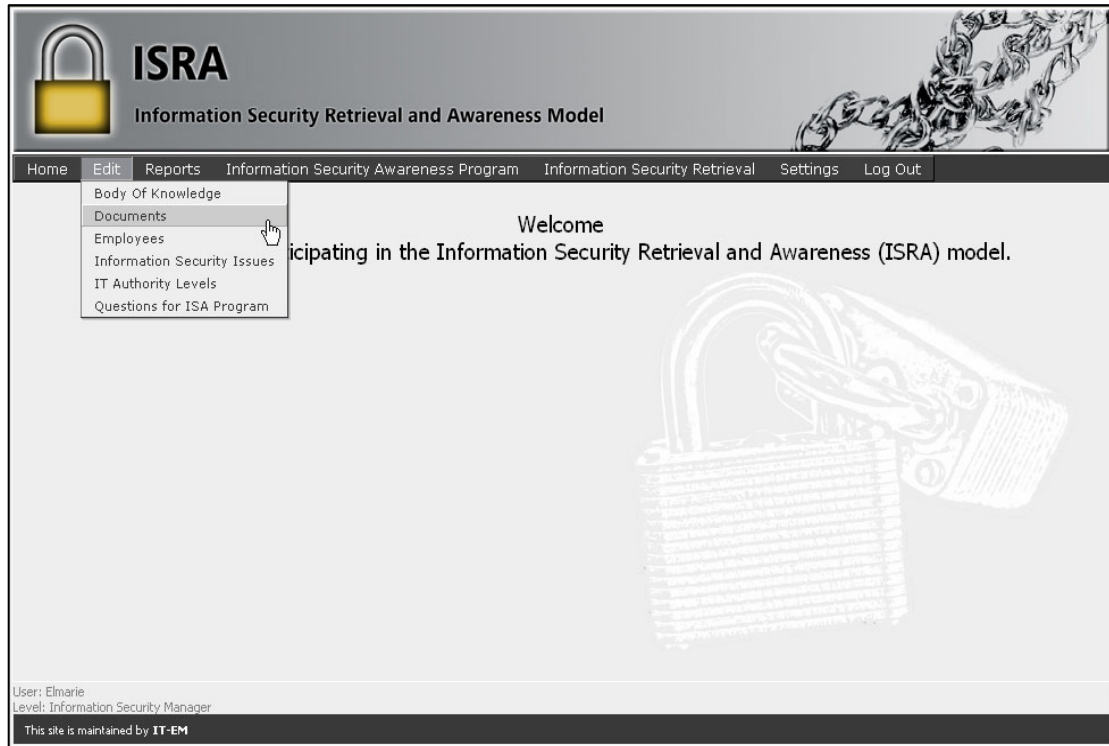


**Figure B12: Confirmation of information to be deleted**

Click on the `Confirm` button at the bottom of the screen to confirm the deletion process. The database will be updated accordingly and the initial screen (depicted in Figure B10) will be displayed again. Alternatively, click on the `Cancel` button to return to the initial screen without deleting the information.

### **B.2.3.2 Documents**

If you want to edit the Information Security documents, click on the `Documents` option under the `Edit` menu option as depicted in Figure B13.



**Figure B13: Edit documents**

After you have clicked on the Documents option, the current Information Security documents on which the Common Body of Knowledge for Information Security is based are displayed, as depicted in Figure B14.



**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Notes:**

- Click on a document to view/ update or delete information on that document
- Click on the Add button to add a Document

< Prev 10 Next 10 >

Document	Location
<a href="#">Board Briefing document on IT Governance</a>	IT Governance Institute, 2001, ISBN 1-893209-27-X
<a href="#">Commonwealth Protective Security Manual</a>	Not Available
<a href="#">Financial Aspects of Corporate Governance report (Cadbury report)</a>	Report of the Committee on the financial Aspect of corporate Governance, (Cadbury report),UK,December 1992
<a href="#">Governance, Control and Audit for Information and Related Technology (COBIT)</a>	IT Governance Institute / ISACA / ISACF, 3rd edition, 2001, ISBN 1-893209-13-X
<a href="#">Information Security Governance: Guidance for Boards of Directors and Executive Management</a>	IT Governance Institute, 2001, ISBN 1-893209-28-8
<a href="#">Information Technology – Guidelines for management of IT Security (GMITS)</a>	ISO/IEC JTC1/SC27, PDTR 13335-1 (revision), version 28-11-2001
<a href="#">International Organization for Standardization Standard 17799 (ISO 17799)</a>	British Standards Institute (BSI), final draft BS7799-2: 2002
<a href="#">IT Infrastructure Library on Security Management</a>	Not Available
<a href="#">National Institute of Standards (NIST) handbook</a>	National Institute of Standards and Technology (NIST), version March 1995
<a href="#">The KING report</a>	Institute of Directors, South Africa, version of July 2001

< Prev 10 Next 10 >

User: Elmarie  
Level: Information Security Manager  
This site is maintained by **IT-EM**

**Figure B14: Current Information Security documents**

To add a new Information Security document, click on the Add button (as depicted in Figure B14). You will then be presented with the screen depicted in Figure B15.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Document**

Name:

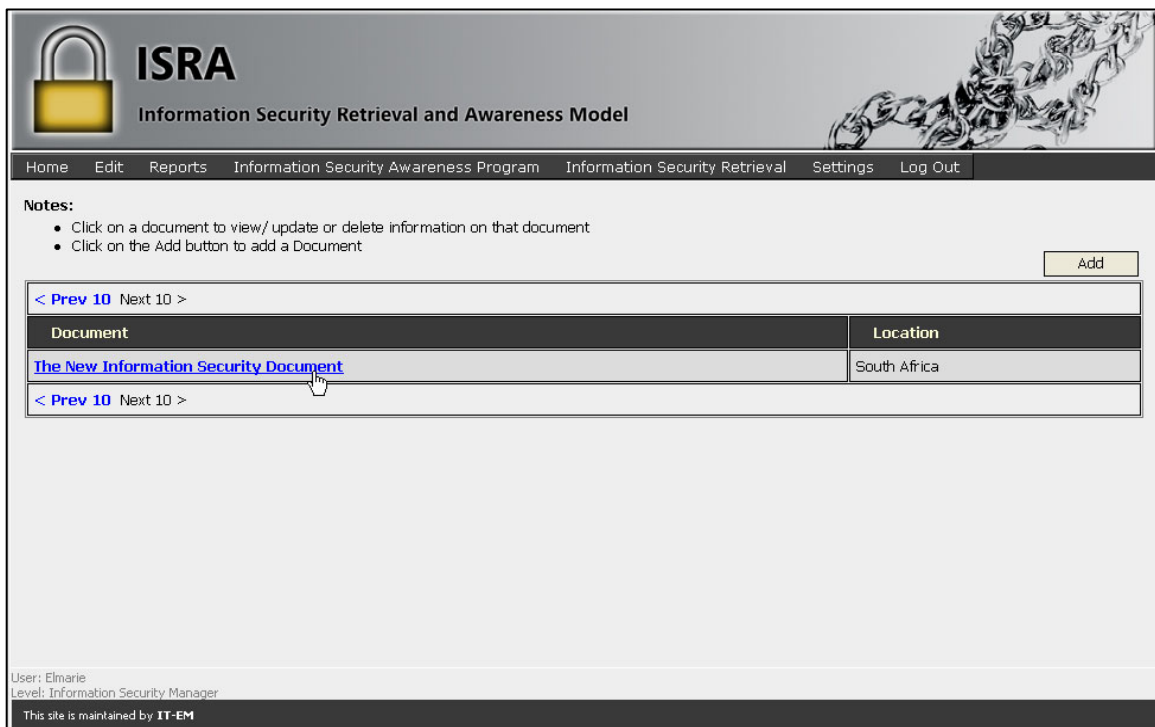
Publication Details:

User: Elmarie  
Level: Information Security Manager  
This site is maintained by **IT-EM**

**Figure B15: Adding a document**

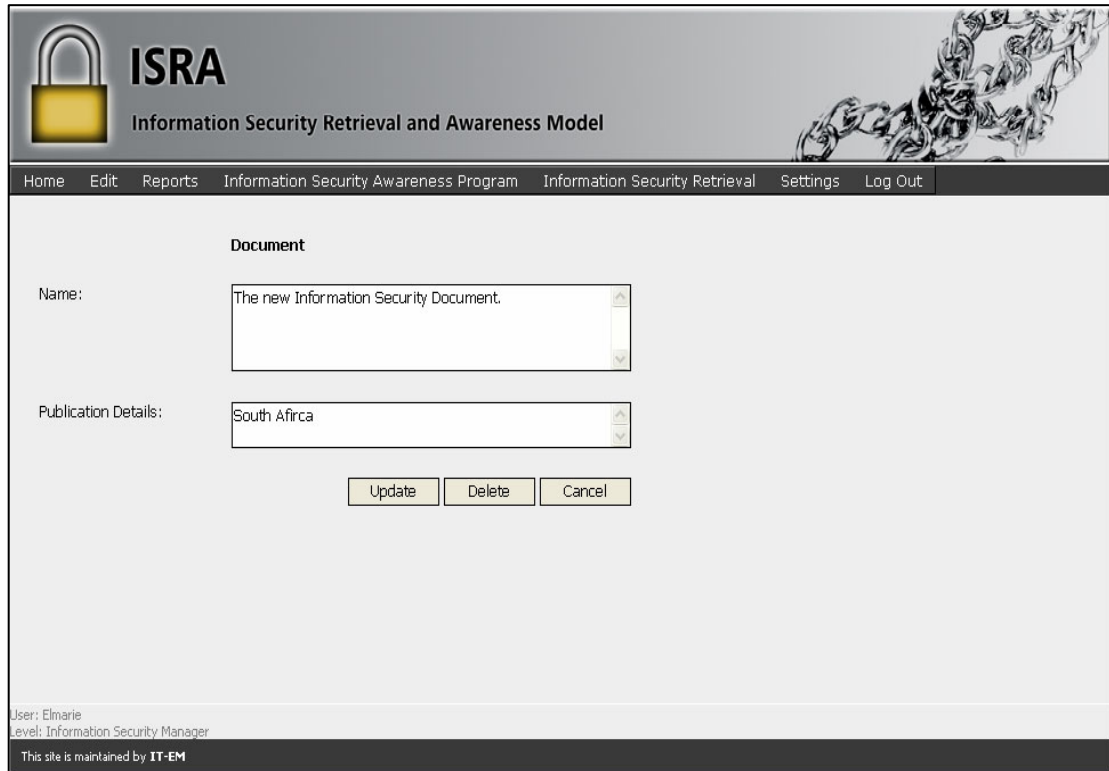
To return to the initial screen (depicted in Figure B14) click on the **Cancel** button at the bottom of the screen. Alternatively, to add a new Information Security document, type the name and publication details of the new document in the appropriate boxes and click on the **Add** button.

The database will now be updated to include this new Information Security document, and the initial screen (Figure B14) will be displayed again. To view the new information added, click on the **Next 10** link in the top or bottom row of the table (depicted in B14) until the new information is displayed. The new information will be displayed as depicted in Figure B16.



**Figure B16: Selecting a document to be updated or deleted**

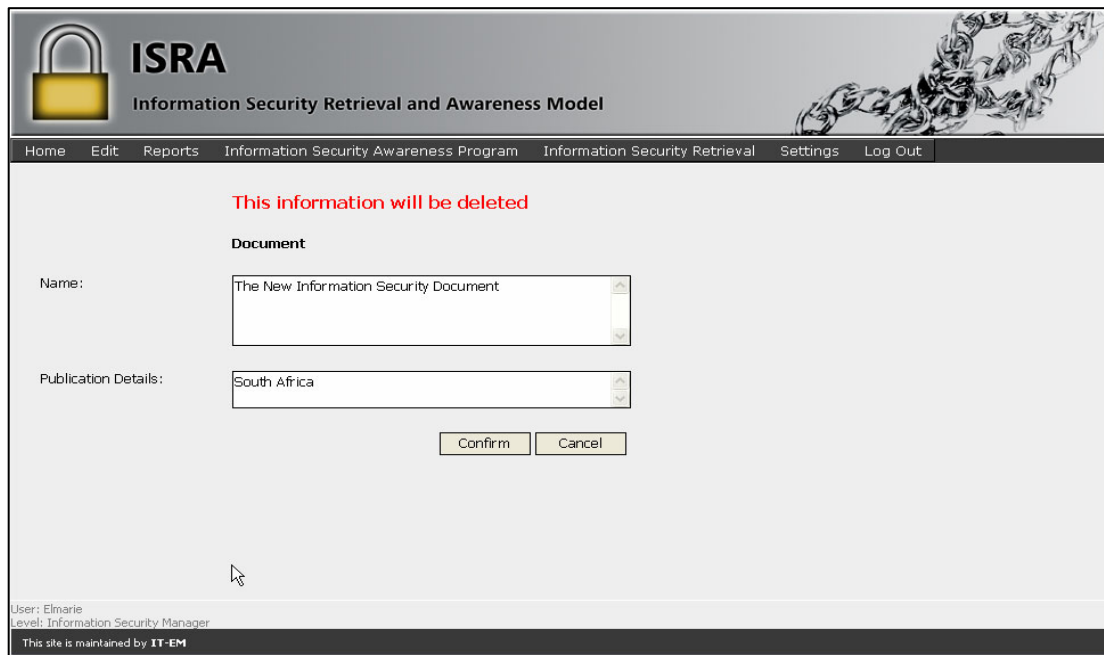
To edit (update or delete) a document, click on the document that you want to edit as displayed in the **Documents** column (see Figure B16). You will subsequently be presented with Figure B17.



**Figure B17: Updating or deleting a document**

You could either update or delete the selected document. If you want to return to the initial screen without deleting the information, click on the `Cancel` button. Alternatively, if you want to update the document, make the necessary changes and click on the `Update` button at the bottom of the screen. The database will then be updated and the initial screen (depicted in Figure B14) will be displayed again.

If you want to delete the document, click on the `Delete` button at the bottom of the screen. The system will prompt you to confirm the `Delete` action. See Figure B18 – top of the screen.

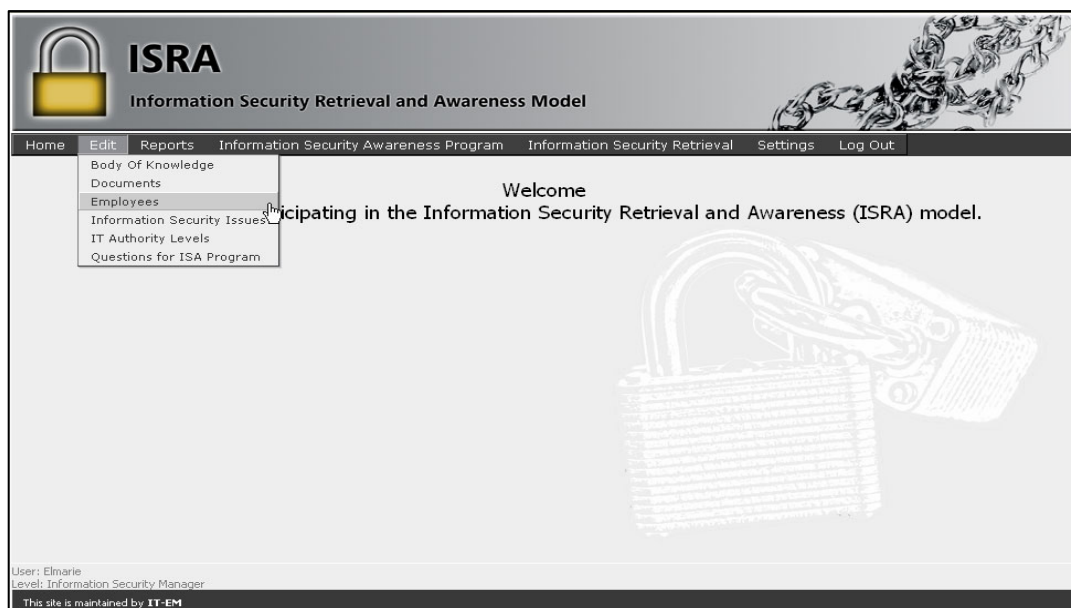


**Figure B18: Confirmation of which document will be deleted**

Click on the **Confirm** button at the bottom of the screen to confirm the deletion process. The database will be updated accordingly and the initial screen (depicted in Figure B14) will be displayed again. Alternatively, click on the **Cancel** button to return to the initial screen without deleting the information.

### B.2.3.3 Employees

If you want to add, edit or delete information on employees, click on the **Employees** option under the **Edit** menu option on the menu bar, as depicted in Figure B19.



**Figure B19: Edit employees**

After you have clicked on the Employees option, information on the current employees is displayed as depicted in Figure B20.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Notes:**

- Click on the surname to view/ update or delete information on that employee
- Click on the Add button to add information on an employee

< Prev 10 Next 10 >

Surname	Name	IT Authority Level
****	***	Executive Management Level
****	****	Board Level
*****	*****	Users
*****	*****	Users
<a href="#">Bouwer</a>	Marais	Information Security Manager
<a href="#">Kritzinger</a>	Elmarie	Information Security Manager

< Prev 10 Next 10 >

User: Elmarie  
Level: Information Security Manager  
This site is maintained by **IT-EM**

*Figure B20: Current employees*

To add information for a new employee, click on the Add button. Figure B21 will be displayed as a result.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

Employee

**Personal Details**

First Name:

Surname:

IT Authority Level:

**User Details**

User Name:

Password:

Confirm Password:

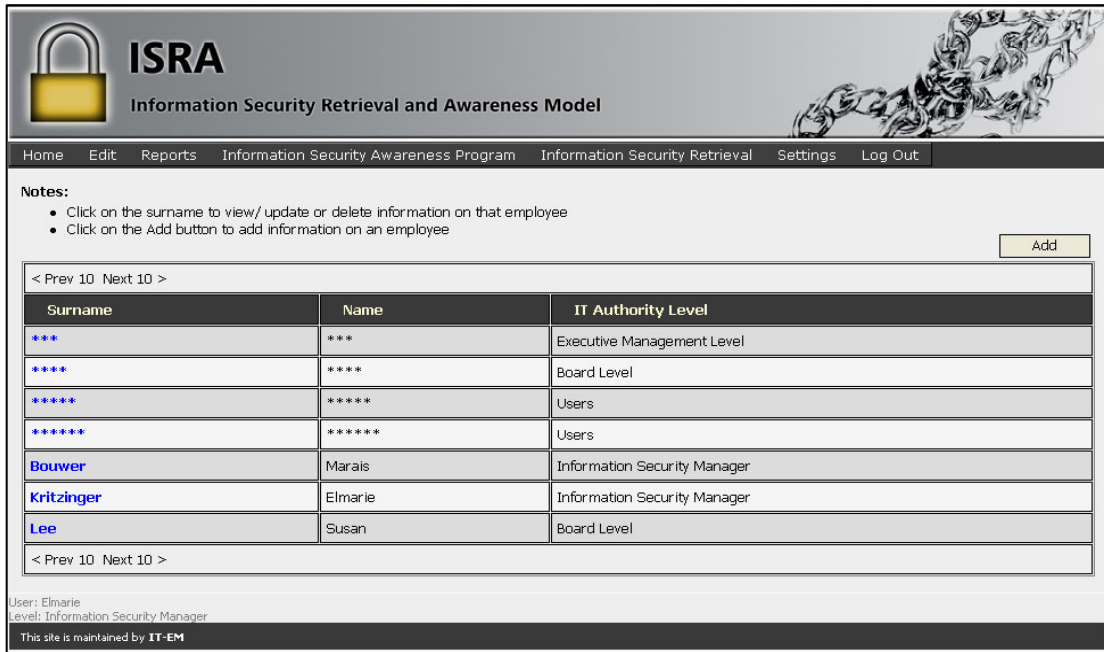
User: Elmarie  
Level: Information Security Manager  
This site is maintained by **IT-EM**

*Figure B21: Adding an employee*

To return to the initial screen (depicted in Figure B14), click on the **Cancel** button at the bottom of the screen. Alternatively, to add a new employee, type the personal details of the employee as well as the user details that are used during the login process in the appropriate boxes. Click on the **Add** button.

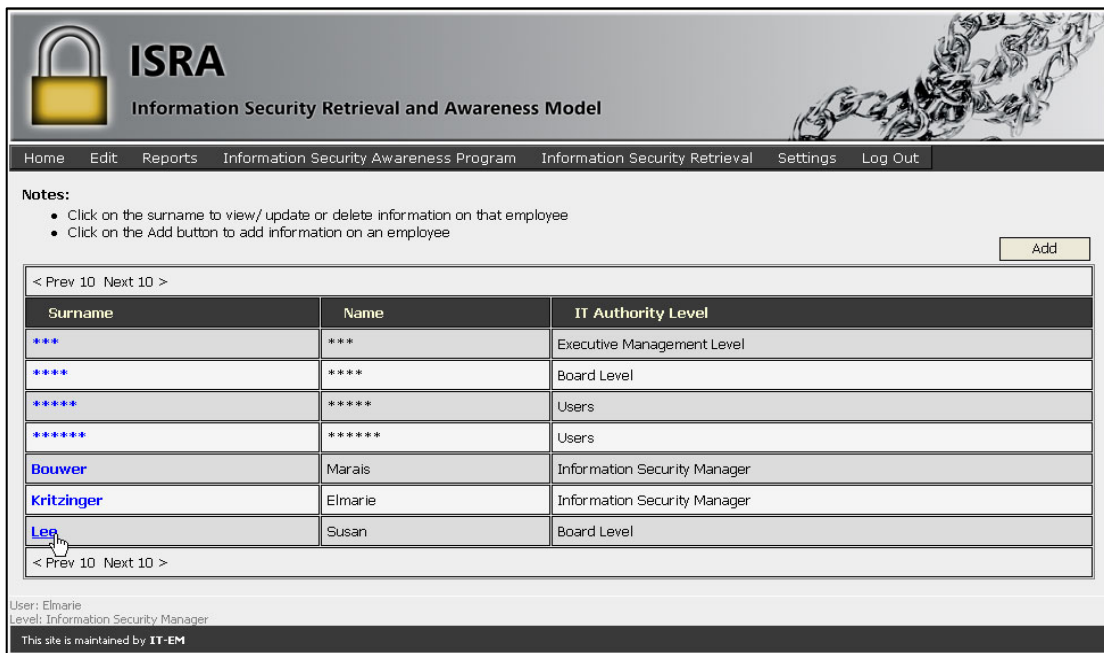
**Figure B22: Adding details on an employee**

The database will now be updated to include information on this new employee, and the initial screen (Figure B14) will be displayed again. To view this new information, click on the **Next 10** link in the top or bottom row of the table if necessary (depicted in B14) until the new information is displayed – the information in the table is stored alphabetically according to surname – as depicted in Figure B23.



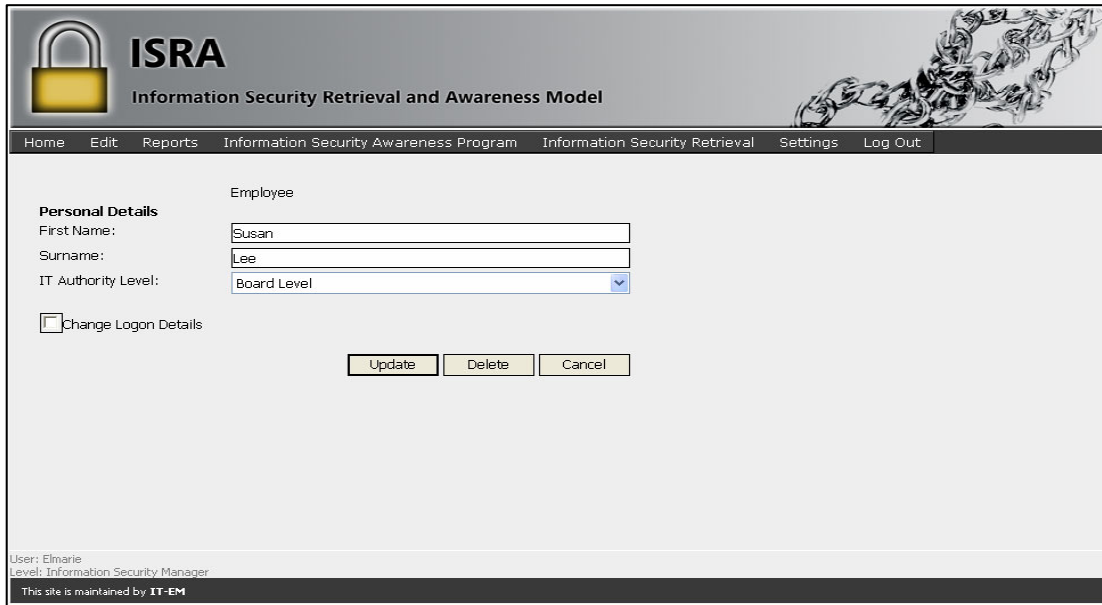
*Figure B23: View information of new employee*

To edit (update or delete) the information on an employee, click on the surname of the employee that you want to edit in the Surname column as indicated in Figure B24.



*Figure B24: Select employee to edit*

You will next be presented with the screen depicted in Figure B25.



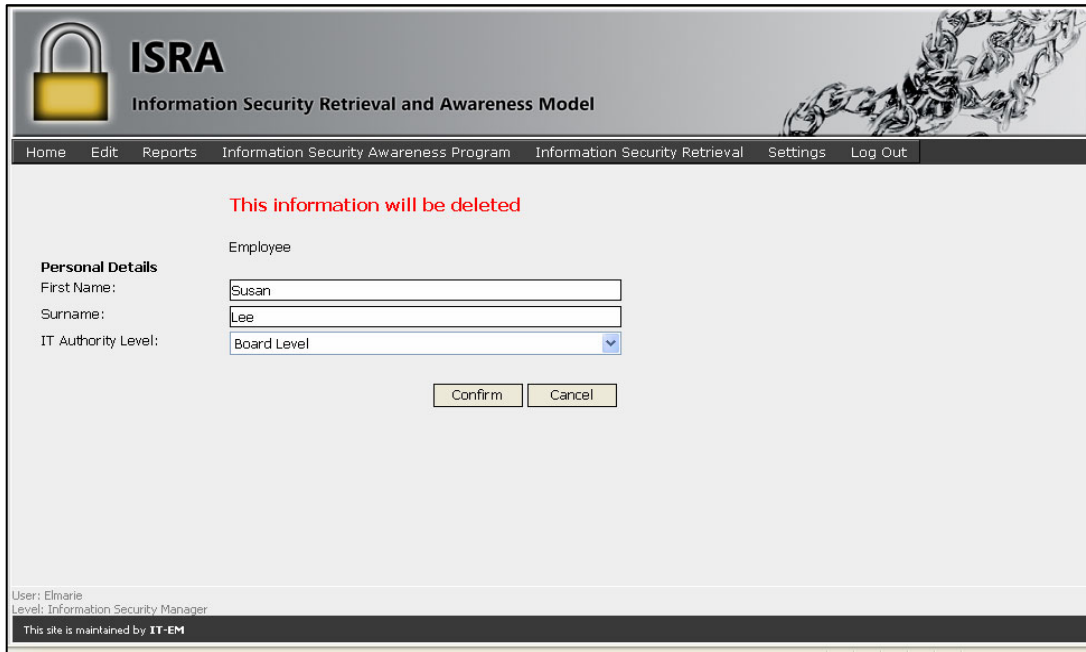
**Figure B25: Updating or deleting an employee**

You could either update or delete information on the selected employee. If you want to return to the initial screen (Figure B14) without updating or deleting the information, click on the `Cancel` button.

Alternatively, if you want to update the employee's details, make the necessary changes in the appropriate boxes of `Personal Details` and click on the `Update` button. If the logon information needs to be updated as well, click on the check box next to `Change Logon Details` and make the necessary changes in the appropriate boxes. The database will then be updated and the initial screen (depicted in Figure B14) will be displayed again.

If you want to delete the employee, click on the `Delete` button. The system will prompt you to confirm the delete action. See Figure B26 – top of the screen.



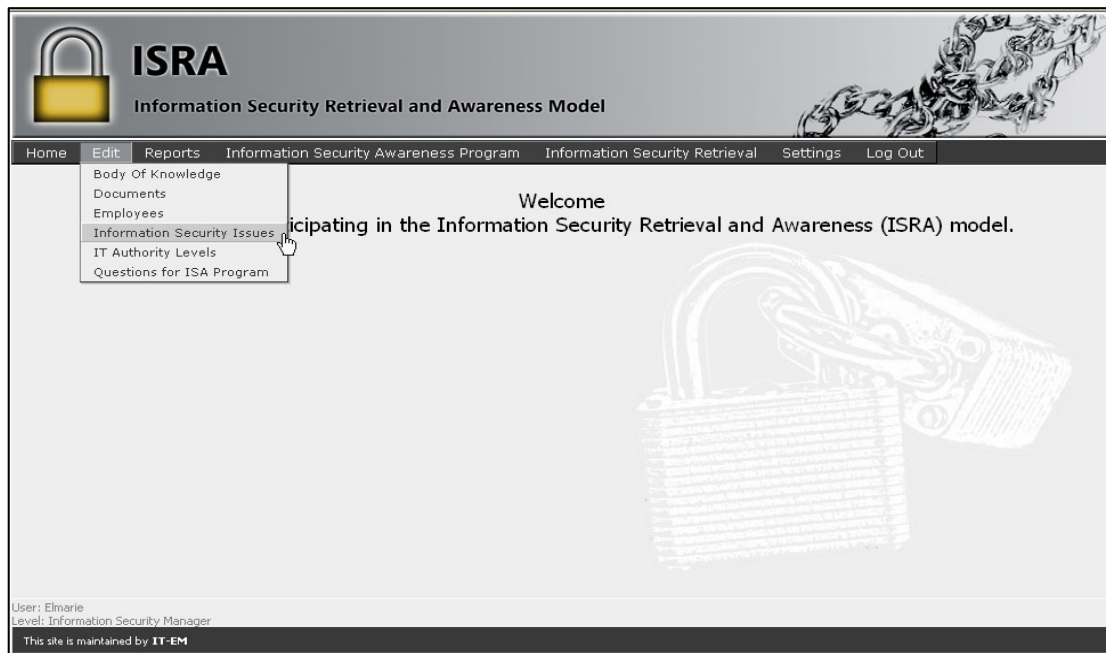


*Figure B26: Confirmation of which employee will be deleted*

Click on the `Confirm` button at the bottom of the screen to confirm the deletion process. The database will be updated accordingly and the initial screen (depicted in Figure B14) will be displayed again. Alternatively, click on the `Cancel` button to return to the initial screen without deleting the information.

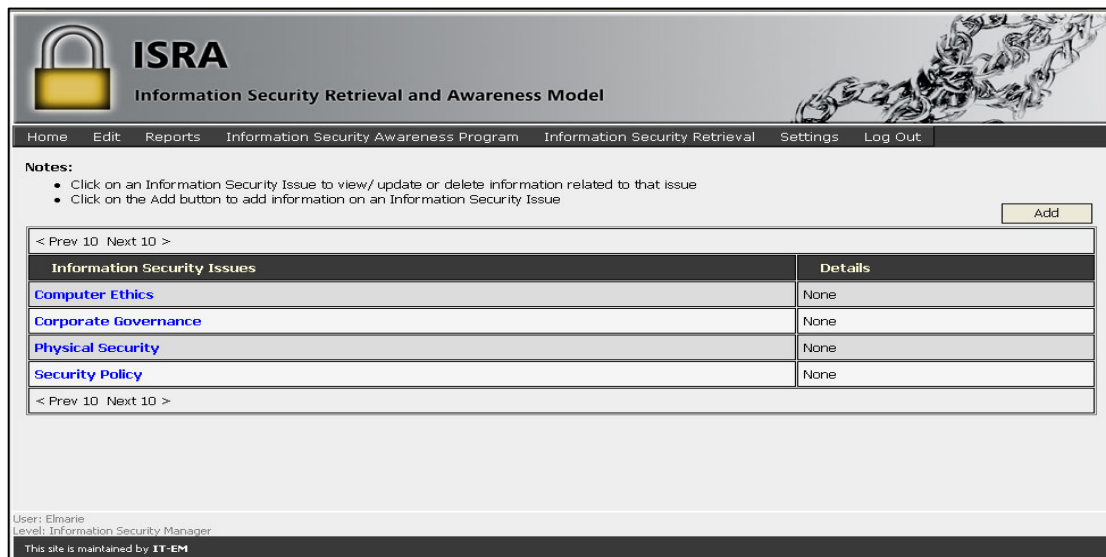
### **B.2.3.4 Information Security Issues**

If you want to add, edit or delete the Information Security issues, click on the `Information Security Issues` option on the menu bar, under the `Edit` menu option as depicted in Figure B27.



**Figure B27: Edit Information Security issues**

After you have clicked on the Information Security Issues option, information is displayed on the Information Security issues for which information is currently stored in the database (see Figure B28).



**Figure B28: Current Information Security issues**

To add information for a new Information Security issue, click on the Add button. Figure B29 will be displayed as a result.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Information Security Issue**

Name:

Details:

Add Cancel

User: Elmarie  
Level: Information Security Manager  
This site is maintained by IT-EM

**Figure B29: Add an Information Security issue**

To return to the initial screen (depicted in Figure B28) click on the `Cancel` button at the bottom of the screen. Alternatively, to add information for a new Information Security issue, type the name and details of the Information Security issue in the appropriate boxes and click on the `Add` button as shown in Figure B30.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Information Security Issue**

Name:

Details:

Add Cancel

User: Elmarie  
Level: Information Security Manager  
This site is maintained by IT-EM

**Figure B30: Adding a new Information Security issue**

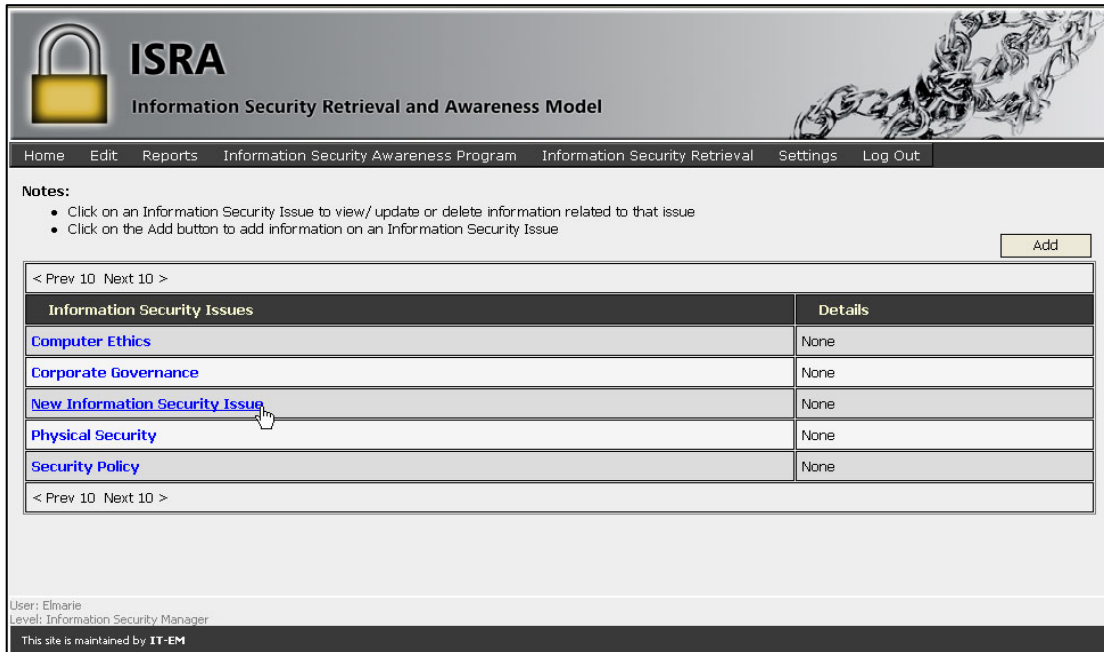
The database will now be updated to include information on this new Information Security issue, and the initial screen (Figure B28) will be displayed again. To view whether this new information has been added, click on the Next 10 link in the top or bottom row of the table if necessary (depicted in B28) until the new information is displayed. The information in the table is stored alphabetically according to the Information Security issues – as depicted in Figure B31.

The screenshot shows the ISRA (Information Security Retrieval and Awareness Model) web application. The header includes the ISRA logo and navigation links: Home, Edit, Reports, Information Security Awareness Program, Information Security Retrieval, Settings, and Log Out. Below the header, there are notes and an 'Add' button. The main content area features a table with two columns: 'Information Security Issues' and 'Details'. The table lists five issues: Computer Ethics, Corporate Governance, New Information Security Issue, Physical Security, and Security Policy, all with 'None' in the Details column. Navigation links '< Prev 10 Next 10 >' are present above and below the table. At the bottom, the user is identified as 'Elmarie' with the level 'Information Security Manager', and a footer note states 'This site is maintained by IT-EM'.

Information Security Issues	Details
<a href="#">Computer Ethics</a>	None
<a href="#">Corporate Governance</a>	None
<a href="#">New Information Security Issue</a>	None
<a href="#">Physical Security</a>	None
<a href="#">Security Policy</a>	None

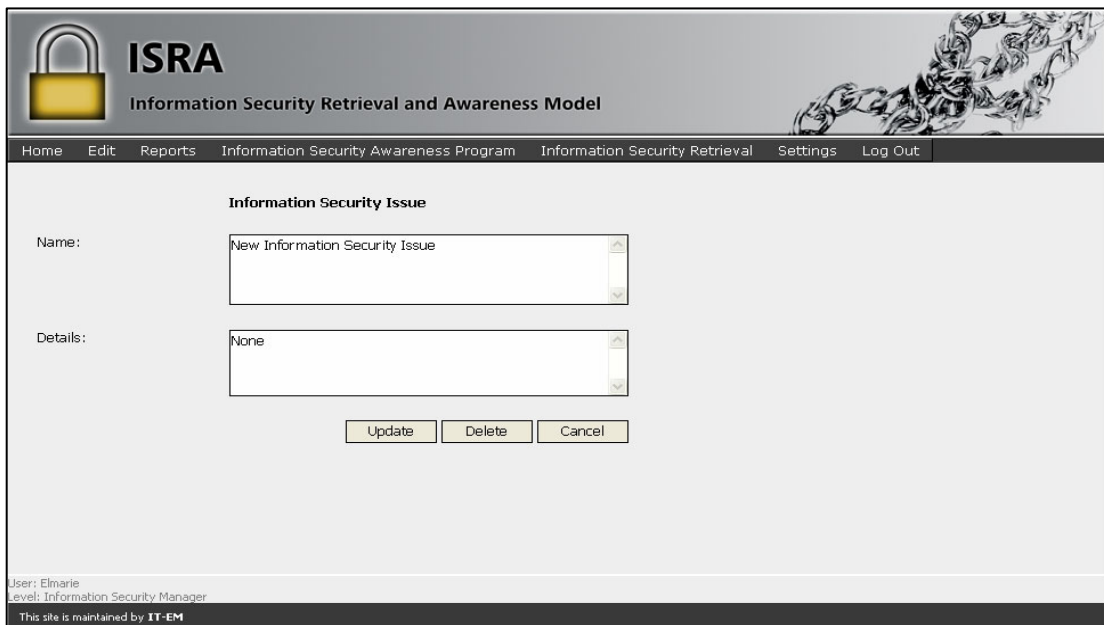
*Figure B31: View Information of new Information Security issue*

To edit (update or delete) an Information Security issue, click the Information Security issue in the Information Security Issue column that you want to edit as indicated in Figure B32.



*Figure B32: Selecting an Information Security issue to edit*

You will accordingly be presented with the screen depicted in Figure B33.

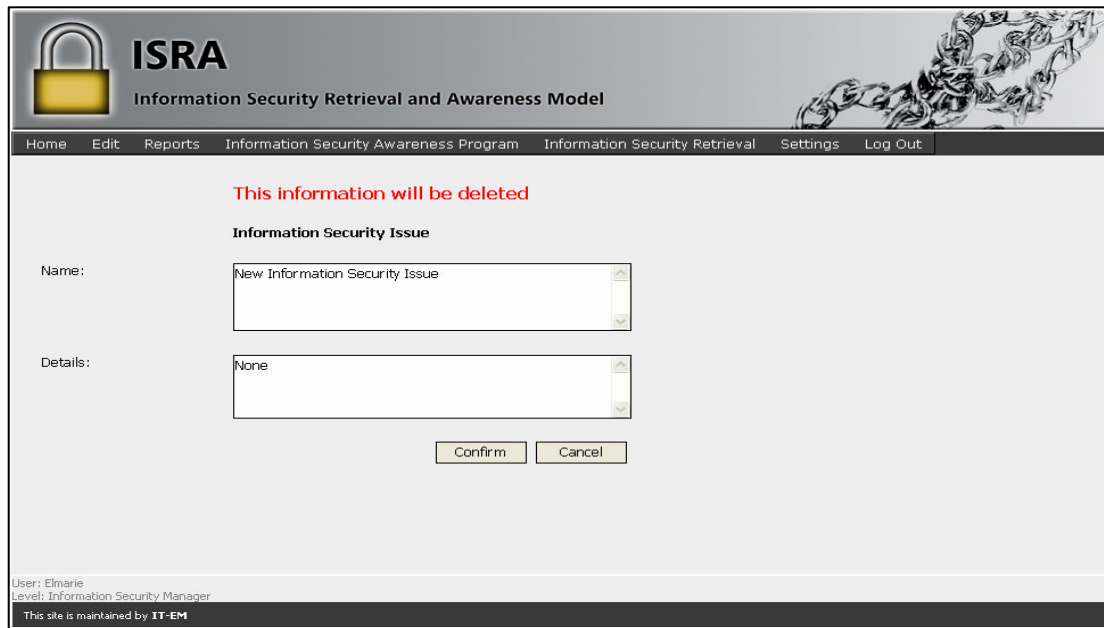


*Figure B33: Update or delete Information Security issues*

You could either update or delete information on the selected Information Security issue. If you want to return to the initial screen (Figure B28) without updating or deleting the information, click on the `Cancel` button.

Alternatively, if you want to update the Information Security issue, make the necessary changes in the appropriate boxes and click on the Update button. The database will be updated and the initial screen depicted in Figure B28 will be displayed again.

If you want to delete the Information Security issue, click on the Delete button at the bottom of the screen. The system will prompt you to confirm the Delete action. See Figure B34 – top of the screen.

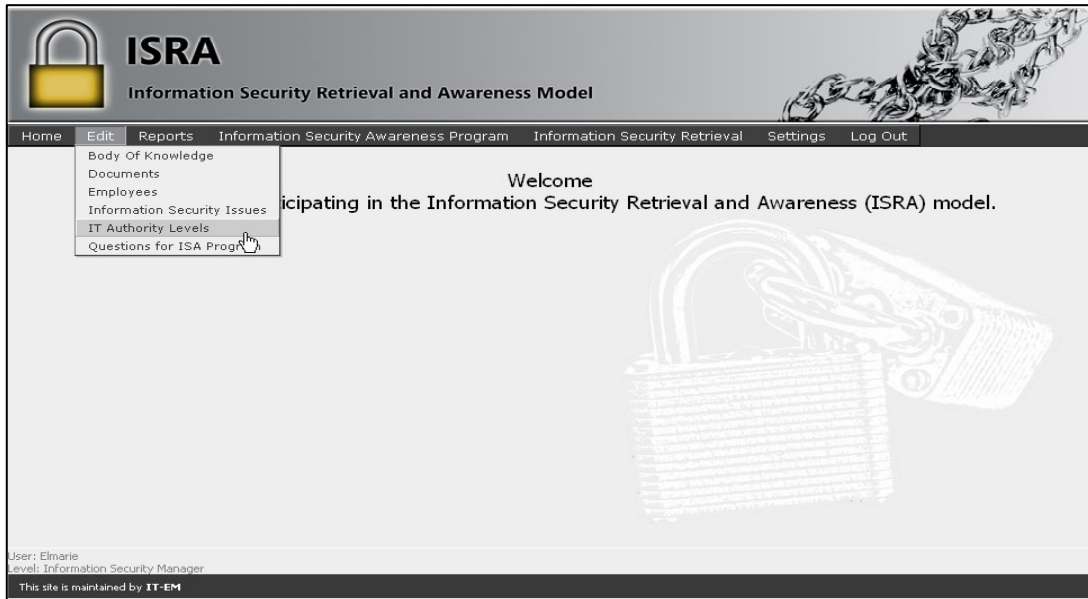


**Figure B34: Confirmation which Information Security issue will be deleted**

Click on the Confirm button at the bottom of the screen to confirm the deletion process. The database will then be updated accordingly and the initial screen (depicted in Figure B28) will be displayed again. Alternatively, click on the Cancel button to return to the initial screen without deleting the information.

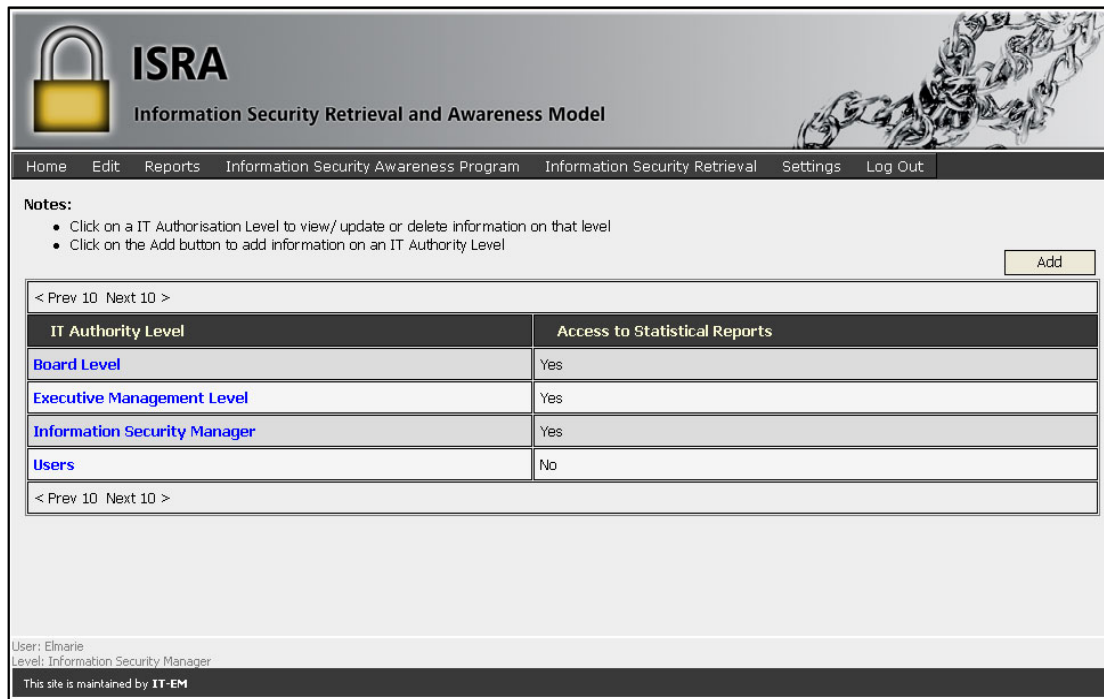
### **B.2.3.5 IT Authority Levels**

If you want to add, edit or delete information on an IT authority level, click on the IT Authority Levels option under the Edit menu option on the menu bar, as depicted in Figure B35.



**Figure B35: Edit IT authority levels**

After you have clicked on the IT Authority Levels option, information on the IT authority levels currently stored in the database is displayed (see Figure B36).



**Figure B36: Current IT authority levels**

To add information for a new IT authority level, click on Add button. Figure B37 will be displayed as a result.

The screenshot shows the ISRA (Information Security Retrieval and Awareness Model) web application interface. At the top left is the ISRA logo, a yellow padlock icon. To its right is the text 'ISRA Information Security Retrieval and Awareness Model'. A navigation menu below the header includes 'Home', 'Edit', 'Reports', 'Information Security Awareness Program', 'Information Security Retrieval', 'Settings', and 'Log Out'. The main content area is titled 'IT Authority Level' and contains two text input fields labeled 'Name:' and 'Details:'. Below these fields is a checkbox labeled 'Allow to access Statistical Reports' which is currently unchecked. At the bottom of the form are two buttons: 'Add' and 'Cancel'. The footer of the page displays 'User: Elmarie', 'Level: Information Security Manager', and 'This site is maintained by IT-EM'.

**Figure B37: Add a new IT authority level**

To return to the initial screen (depicted in Figure B36) without adding the information, click on the `Cancel` button at the bottom of the screen. Alternatively, to add information on a new IT authority level, type the name and details of the new IT authority level in the appropriate boxes. Click on the check box next to `Allow to access Statistical Reports` if appropriate. Then click on the `Add` button as depicted in Figure B38.

This screenshot shows the same 'IT Authority Level' form as Figure B37, but with data entered. The 'Name:' field contains the text 'New IT Authority Level' and the 'Details:' field contains the text 'None'. The 'Allow to access Statistical Reports' checkbox is now checked. The 'Add' and 'Cancel' buttons remain at the bottom. The footer information is identical to the previous screenshot.

**Figure B38: Adding an IT authority level**



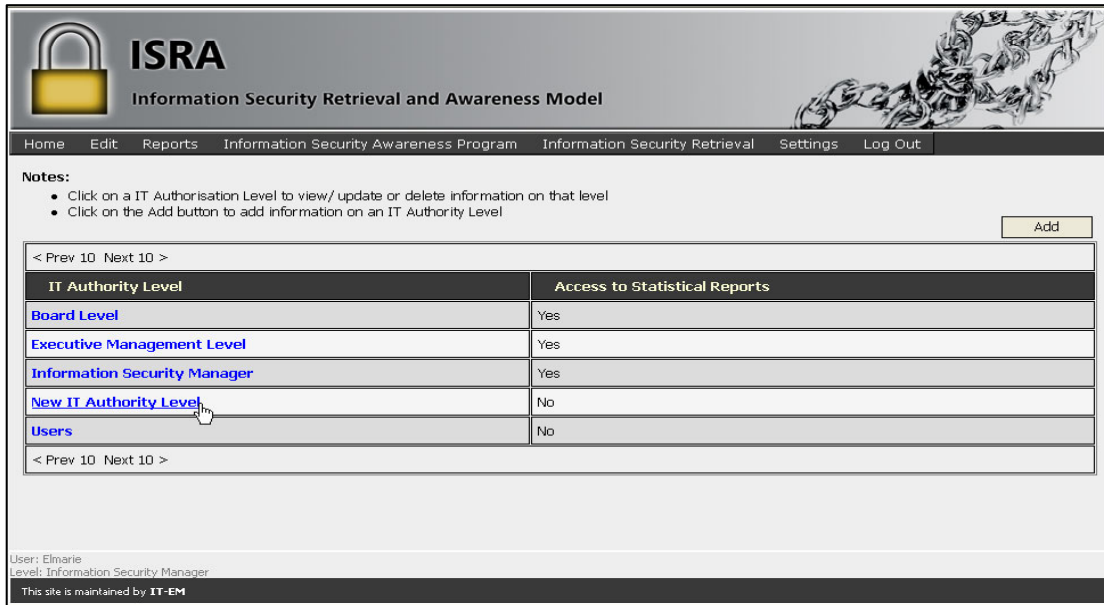
The database will now be updated to include information on this new IT authority level, and the initial screen (Figure B36) will be displayed again. To view this information, click on the `Next 10` link in the top or bottom row of the table if necessary until the new information is displayed. The information in the table is sorted alphabetically according to the IT authority level – see Figure B39.

The screenshot shows the ISRA (Information Security Retrieval and Awareness Model) web application. The header includes the ISRA logo and a navigation menu with links for Home, Edit, Reports, Information Security Awareness Program, Information Security Retrieval, Settings, and Log Out. Below the header, there are notes and an 'Add' button. The main content area features a table with two columns: 'IT Authority Level' and 'Access to Statistical Reports'. The table lists five authority levels: Board Level, Executive Management Level, Information Security Manager, New IT Authority Level, and Users. The 'Access to Statistical Reports' column shows 'Yes' for the first three levels and 'No' for the last two. Navigation links '< Prev 10 Next 10 >' are present above and below the table. At the bottom, the user is identified as 'Elmarie' with the role 'Information Security Manager', and a footer note states 'This site is maintained by IT-EM'.

IT Authority Level	Access to Statistical Reports
<a href="#">Board Level</a>	Yes
<a href="#">Executive Management Level</a>	Yes
<a href="#">Information Security Manager</a>	Yes
<a href="#">New IT Authority Level</a>	No
<a href="#">Users</a>	No

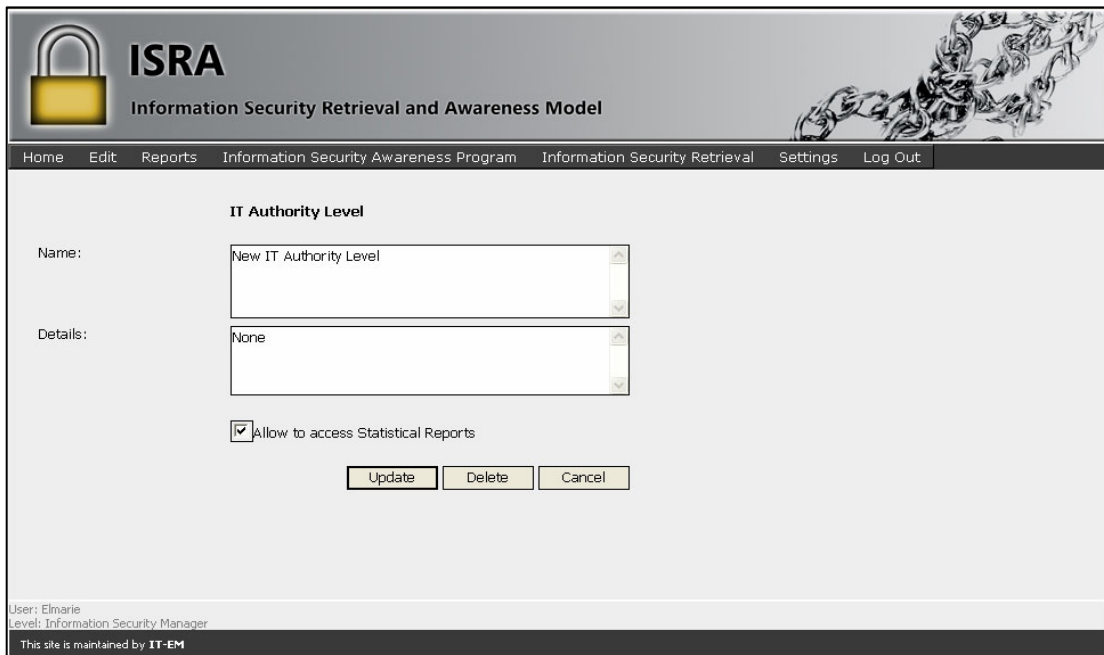
**Figure B39: View information of new IT authority level**

To edit (update or delete) an IT authority level, click the IT authority level in the `IT Authority Level` column that you want to edit (as indicated in Figure B40.)



**Figure B40: Selecting an IT authority level to edit**

You will subsequently be presented with the screen depicted in Figure A41.

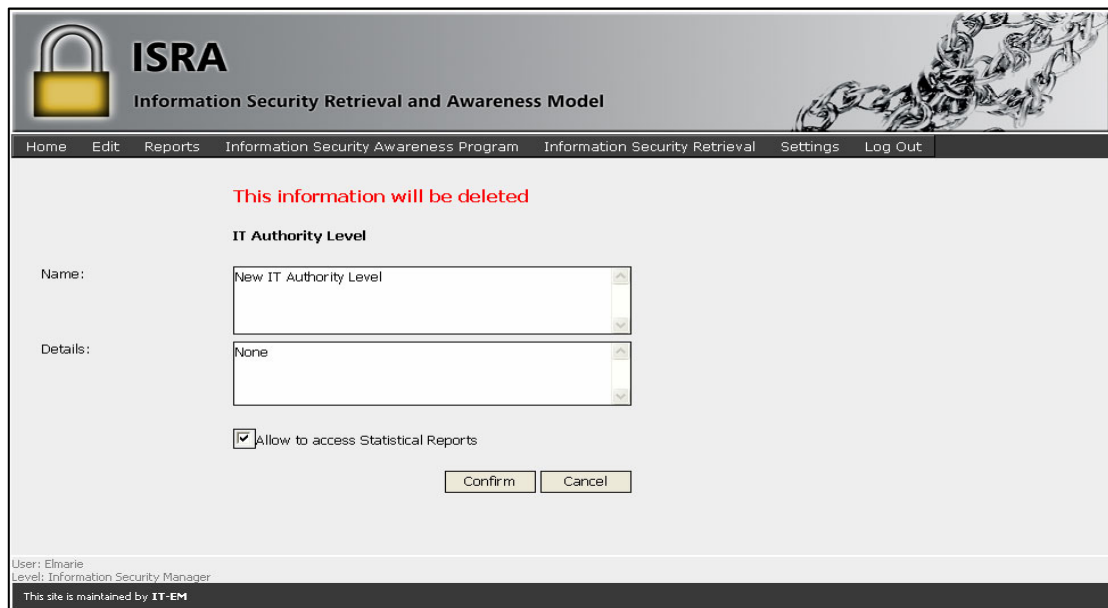


**Figure B41: Updating or deleting an IT authority level**

You could either update or delete information on the selected IT authority level. If you want to return to the initial screen (Figure B36) without updating or deleting the information, click on the `Cancel` button.

Alternatively, if you want to update information on the IT authority level, make the necessary changes in the appropriate boxes and click on the Update button. The database will be updated and the initial screen (depicted in Figure B36) will be displayed again.

If you want to delete information on the IT authority level, click on the Delete button at the bottom of the screen. The system will prompt you to confirm the Delete action. See Figure B42 – top of the screen.

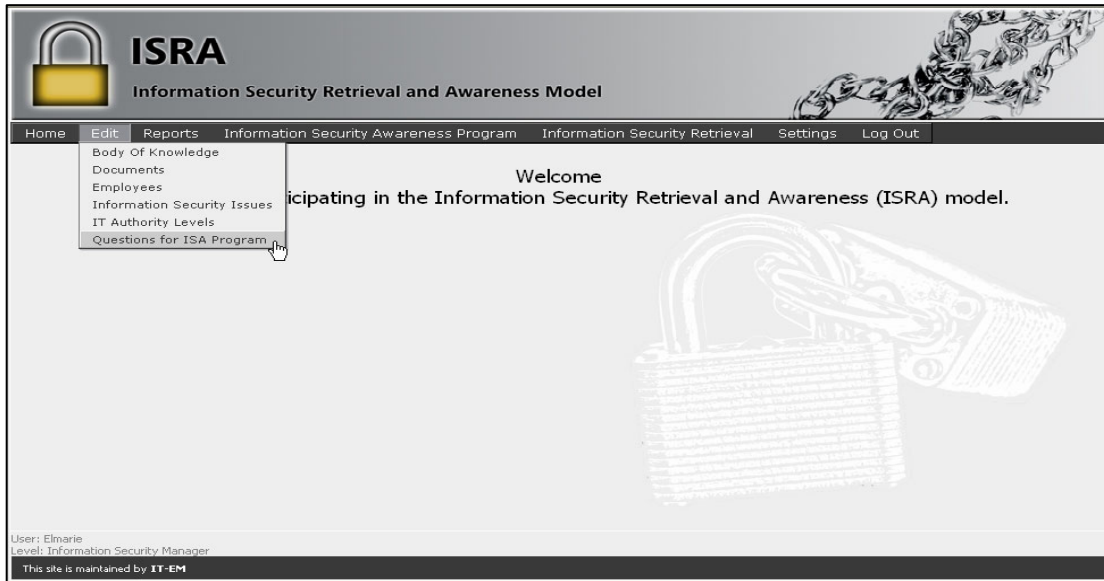


**Figure B42: Confirmation of the IT authority level to be deleted**

Click on the Confirm button at the bottom of the screen to confirm the deletion process. The database will be updated accordingly and the initial screen (depicted in Figure B36) will be displayed again. Alternatively, click on the Cancel button to return to the initial screen without deleting the information.

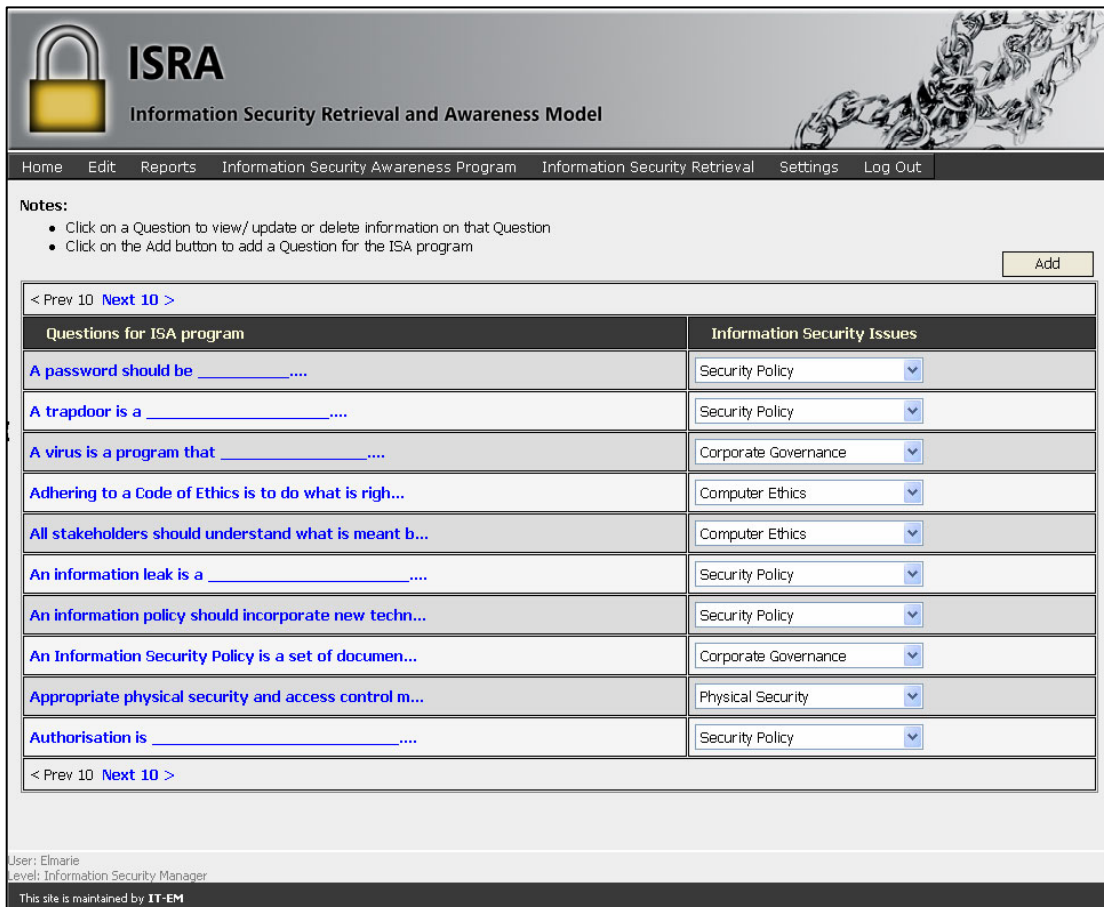
### **B.2.3.6 Questions for ISA Program**

If you want to add or delete information on questions for the Information Security Awareness Program, click on the Questions for ISA Program option under the Edit menu option on the menu bar, as depicted in Figure B43.



**Figure B43: Question for Information Security awareness program**

After you have clicked on the Questions for ISA Program option, the questions for the Information Security awareness program that are currently stored in the database will be displayed as depicted in Figure B44.



**Figure B44: Information Security awareness questions**

To add a new question, click on the **Add** button. Figure B45 will be displayed as a result.

**Figure B45: Add a new question**

To return to the initial screen (depicted in Figure B44), click on the **Cancel** button at the bottom of the screen. Alternatively, to add new questions, type your question in the **Question** text box. The user will select the correct answer from a list of answers. Type a possible answer in the **Answer** text box and click on the check box next to **Correct Answer** if appropriate (see Figure B46). A tick mark will appear in the box when you click. To remove such a tick mark, just click on it again and it will disappear.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Question**

Question: An Information Security Policy is important.

Answer: True

Correct Answer

Answers to Question:

IT Authority Levels:

- Board Level
- Executive Management Level
- Information Security Manager
- Users

Information Security Issues:

- Computer Ethics
- Corporate Governance
- Physical Security
- Security Policy

User: Elmarie  
Level: Information Security Manager  
This site is maintained by IT-EM

***Figure B46: Adding a new question and answers for the Information Security awareness program***

To add another answer, click on the Add button to the right of the Answer text box. The screen will be updated to display the list of possible answers for this question so far – see Figure B47.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Question**

Question:

Answer:

Correct Answer

Answers to Question:

Answer	Correct Answer
True	True

IT Authority Levels:

- Board Level
- Executive Management Level
- Information Security Manager
- Users

Information Security Issues:

- Computer Ethics
- Corporate Governance
- Physical Security
- Security Policy

User: Elmarie  
Level: Information Security Manager  
This site is maintained by IT-EM

*Figure B47: Adding a correct answer*

Type another possible answer in the Answer text box and click on the check box next to Correct Answer if appropriate. Note that only **one** answer can be correct. If you select more than one answer to be correct, you will be presented with the warning message displayed below the Answer text box after you have clicked the Add button (see Figure B48).

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Question**

Question: An Information Security Policy is important.

Answer: False

**Only one answer can be true**

Correct Answer

Answers to Question:

Answer	Correct Answer
True	True

IT Authority Levels:

- Board Level
- Executive Management Level
- Information Security Manager
- Users

Information Security Issues:

- Computer Ethics
- Corporate Governance
- Physical Security
- Security Policy

User: Elmarie  
Level: Information Security Manager

This site is maintained by IT-EM

**Figure B48: Warning about correct answer**

To continue, remove the tick from the check box next to the **Correct Answer** label by clicking on it. Then click on the **Add** button again to add the answer. The screen will be updated to include this answer as well. Once you have added all possible answers for this question, continue to select the relevant IT authority levels. Click on the check boxes next to the specific **IT Authority Level** that needs to be aware of this information. A tick mark will appear in each box when you click. To remove such a tick mark, just click on it again and it will disappear. The next step is to indicate the Information Security issue that is assessed in this new question. Therefore, click on the check boxes next to each Information Security issue that is assessed in this question. Click on the **Add**



button (at the bottom of the screen) to add the new question with its possible answers to the database.

If you fail to click on the appropriate IT Authority Levels and Information Security Issues check boxes, you will be presented with a message on the screen indicating that one or more IT authority levels and Information Security issues are required (see Figure B49).

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Question**

Question:

Answer:

Correct Answer

Answers to Question:

Answer	Correct Answer
True	True
False	False

IT Authority Levels: **Required**

- Board Level
- Executive Management Level
- Information Security Manager
- Users

Information Security Issues: **Required**

- Computer Ethics
- Corporate Governance
- Physical Security
- Security Policy

User: Elmarie  
Level: Information Security Manager  
This site is maintained by IT-EM

**Figure B49: Warning to fill in required issues**

To continue, enter the necessary information (as depicted in Figure B50) and click the Add button at the bottom of the screen.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Question**

Question:

Answer:

Correct Answer

Answers to Question:

Answer	Correct Answer
True	True
False	False

IT Authority Levels:

- Board Level
- Executive Management Level
- Information Security Manager
- Users

Information Security Issues:

- Computer Ethics
- Corporate Governance
- Physical Security
- Security Policy

User: Elmarie  
Level: Information Security Manager

This site is maintained by IT-EM

**Figure B50: Add a new Information Security awareness question**

The database will now be updated to include information on this new question, and the initial screen (Figure B44) will be displayed again. To view this new information, click on the Next 10 link in the top or bottom row of the table if necessary until this information is displayed. The information in the table is stored alphabetically – as depicted in Figure B51.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Notes:**

- Click on a Question to view/ update or delete information on that Question
- Click on the Add button to add a Question for the ISA program

< Prev 10 Next 10 >

Questions for ISA program	Information Security Issues
<a href="#">A password should be _____</a>	Security Policy
<a href="#">A trapdoor is a _____</a>	Security Policy
<a href="#">A virus is a program that _____</a>	Corporate Governance
<a href="#">Adhering to a Code of Ethics is to do what is righ...</a>	Computer Ethics
<a href="#">All stakeholders should understand what is meant b...</a>	Computer Ethics
<a href="#">An information leak is a _____</a>	Security Policy
<a href="#">An information policy should incorporate new techn...</a>	Security Policy
<a href="#">An Information Security Policy is a set of documen...</a>	Corporate Governance
<a href="#">An Information Security Policy is important....</a>	Security Policy
<a href="#">Appropriate physical security and access control m...</a>	Physical Security

< Prev 10 Next 10 >

User: Elmarie  
Level: Information Security Manager  
This site is maintained by IT-EM

**Figure B51: View information on the new Information Security awareness question**

To delete an Information Security awareness question, click on the question to be deleted in the Questions for ISA program column as indicated in Figure B52.

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Notes:**

- Click on a Question to view/ update or delete information on that Question
- Click on the Add button to add a Question for the ISA program

< Prev 10 Next 10 >

Questions for ISA program	Information Security Issues
<a href="#">A password should be _____</a>	Security Policy
<a href="#">A trapdoor is a _____</a>	Security Policy
<a href="#">A virus is a program that _____</a>	Corporate Governance
<a href="#">Adhering to a Code of Ethics is to do what is righ...</a>	Computer Ethics
<a href="#">All stakeholders should understand what is meant b...</a>	Computer Ethics
<a href="#">An information leak is a _____</a>	Security Policy
<a href="#">An information policy should incorporate new techn...</a>	Security Policy
<a href="#">An Information Security Policy is a set of documen...</a>	Corporate Governance
<a href="#">An Information Security Policy is important....</a>	Security Policy
<a href="#">Appropriate physical security and access control m...</a>	Physical Security

< Prev 10 Next 10 >

User: Elmarie  
Level: Information Security Manager  
This site is maintained by IT-EM

**Figure B52: Selecting an Information Security awareness question to be deleted**

You will next be presented with the detailed information regarding the question as depicted in Figure B53.

The screenshot shows the ISRA web application interface. At the top left is the ISRA logo (a padlock) and the text "ISRA Information Security Retrieval and Awareness Model". A navigation menu includes Home, Edit, Reports, Information Security Awareness Program, Information Security Retrieval, Settings, and Log Out. The main content area is titled "Question" and contains the following elements:

- Question:** A text box containing "An Information Security Policy is important."
- Answers to Question:** A table with two columns: "Answer" and "Correct Answer".
 

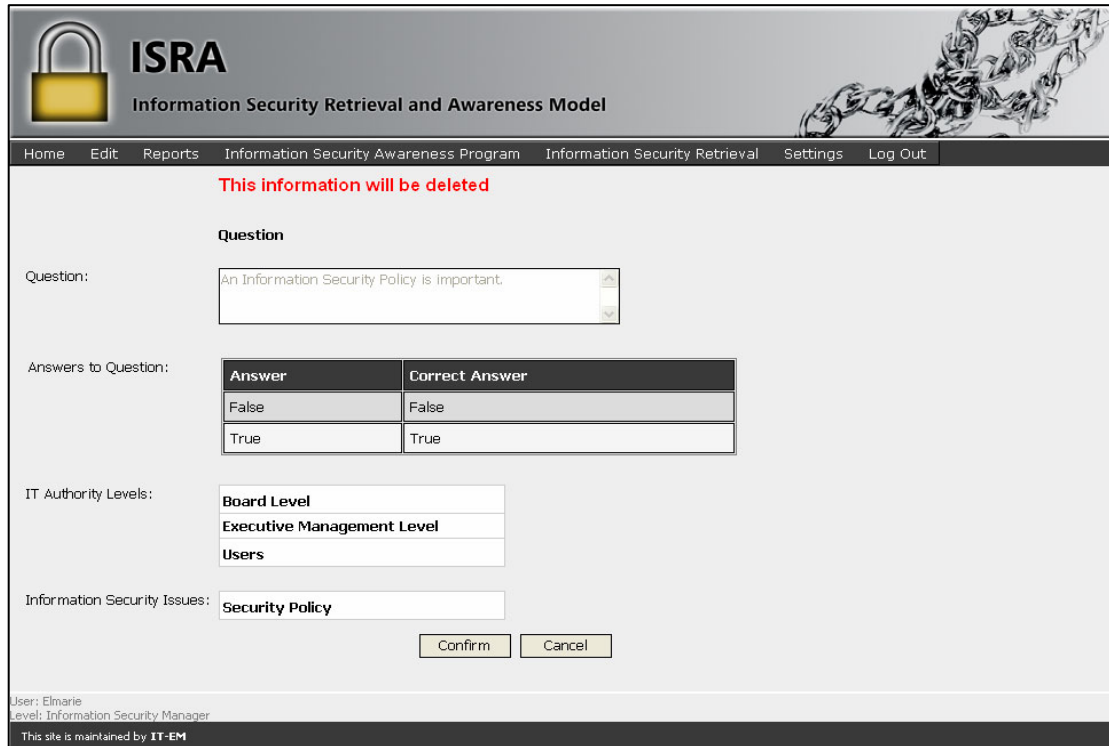
Answer	Correct Answer
False	False
True	True
- IT Authority Levels:** A list box containing "Board Level", "Executive Management Level", and "Users".
- Information Security Issues:** A text box containing "Security Policy".

At the bottom of the form are two buttons: "Cancel" and "Delete". The footer of the page displays "User: Elmarie", "Level: Information Security Manager", and "This site is maintained by IT-EM".

**Figure B53: View current Information Security question**

If you want to return to the initial screen without deleting the information, click on the **Cancel** button.

Alternatively, if you want to delete the question, click on the **Delete** button at the bottom of the screen. The system will prompt you to confirm the Delete action. See Figure B54 – top of the screen.

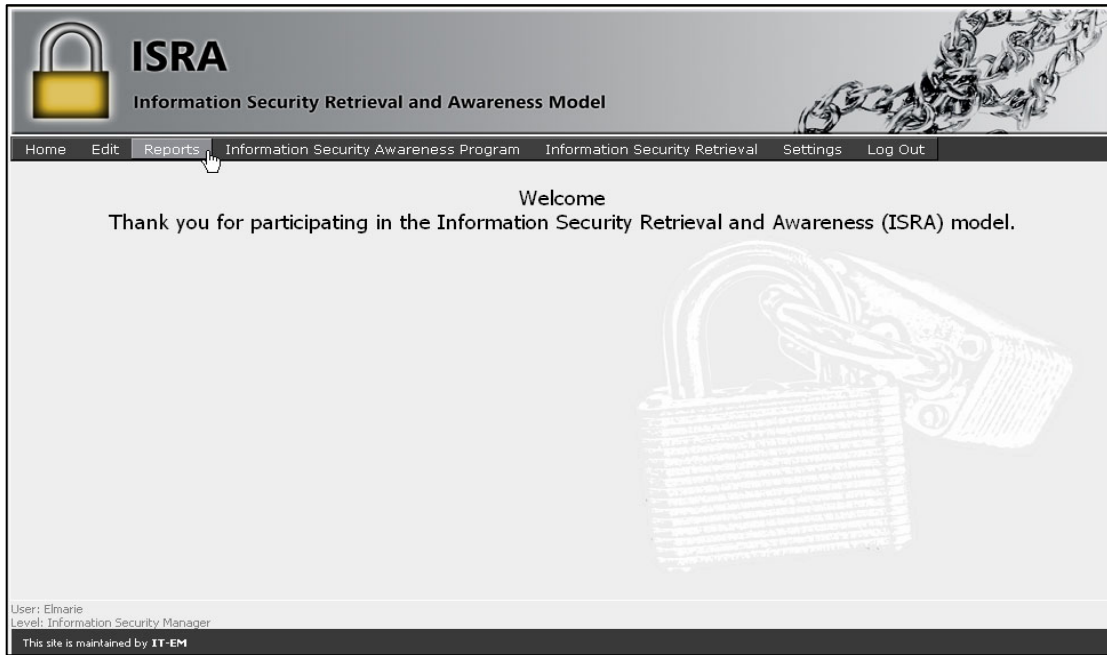


*Figure B54: Confirmation of deletion process*

Click on the `Confirm` button at the bottom of the screen to confirm the deletion process. The database will then be updated and the initial screen (depicted in Figure B44) will be displayed again. Alternatively, click on the `Cancel` button to return to the initial screen without deleting the information.

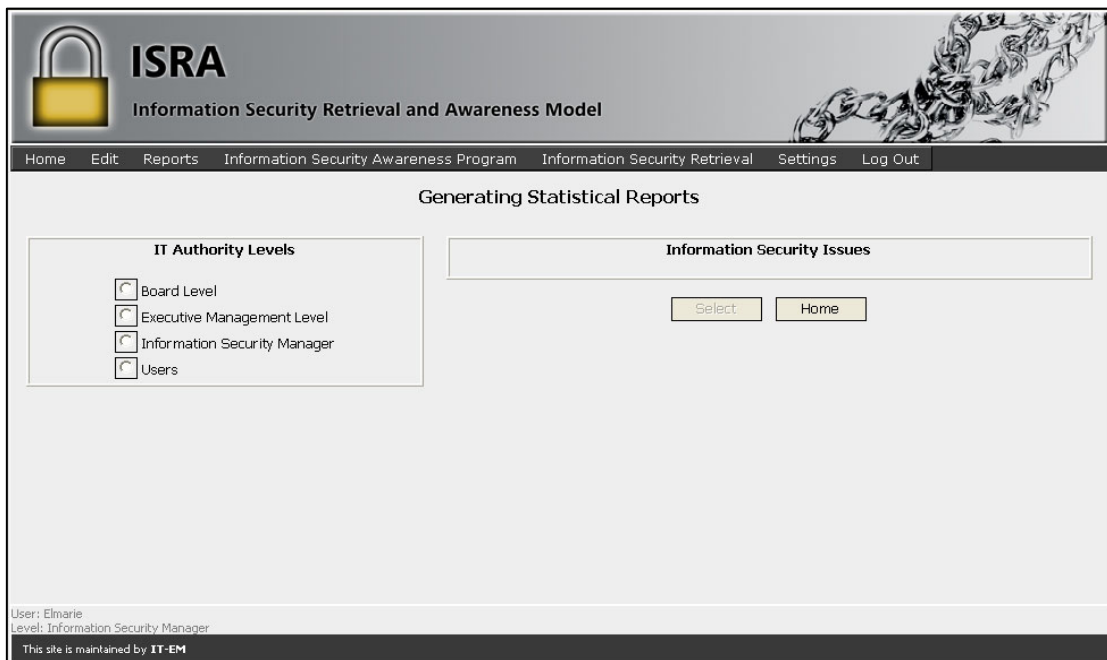
### **B3.4 Report function**

If you want to generate a report, click on the `Report` option on the menu bar as depicted in Figure B55.



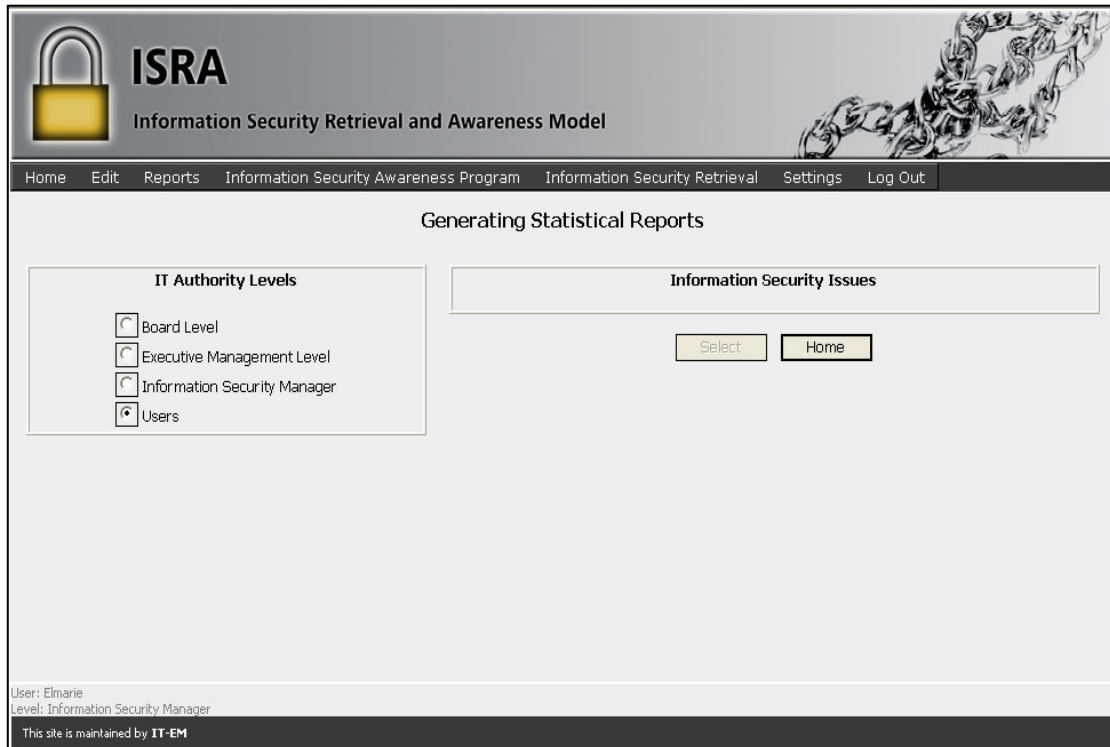
*Figure B55: Report option*

You will be presented with the screen that is depicted Figure B56.



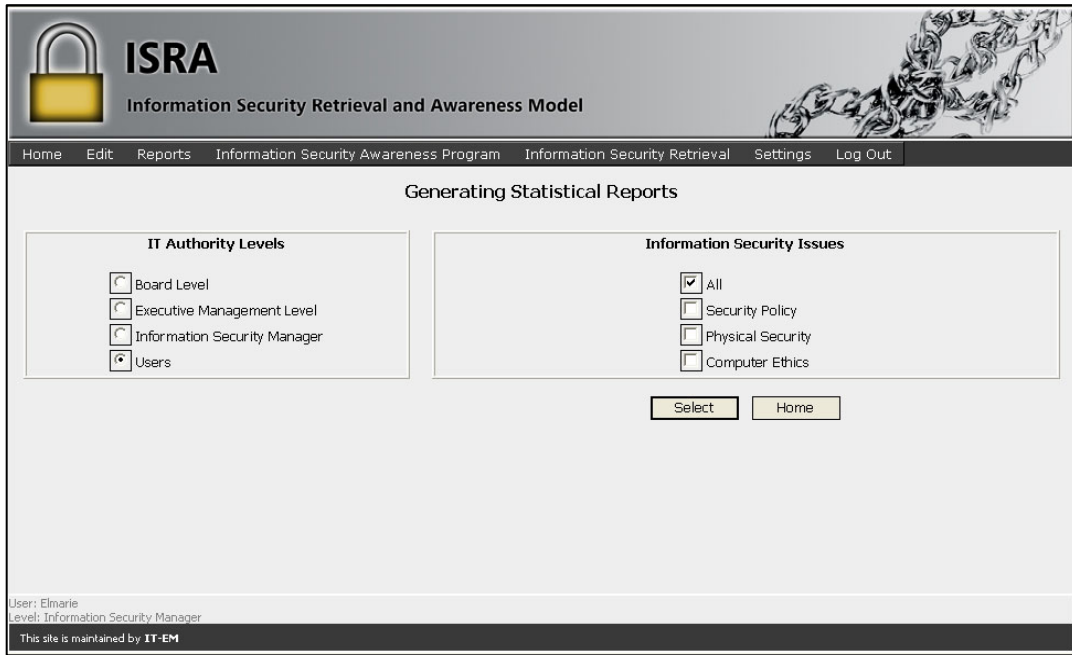
*Figure B56: Selecting an IT authority level*

Select an IT authority level on which you want to generate the report by clicking on the appropriate radio button as indicated in Figure B57.



**Figure B57: Selecting an IT authority level**

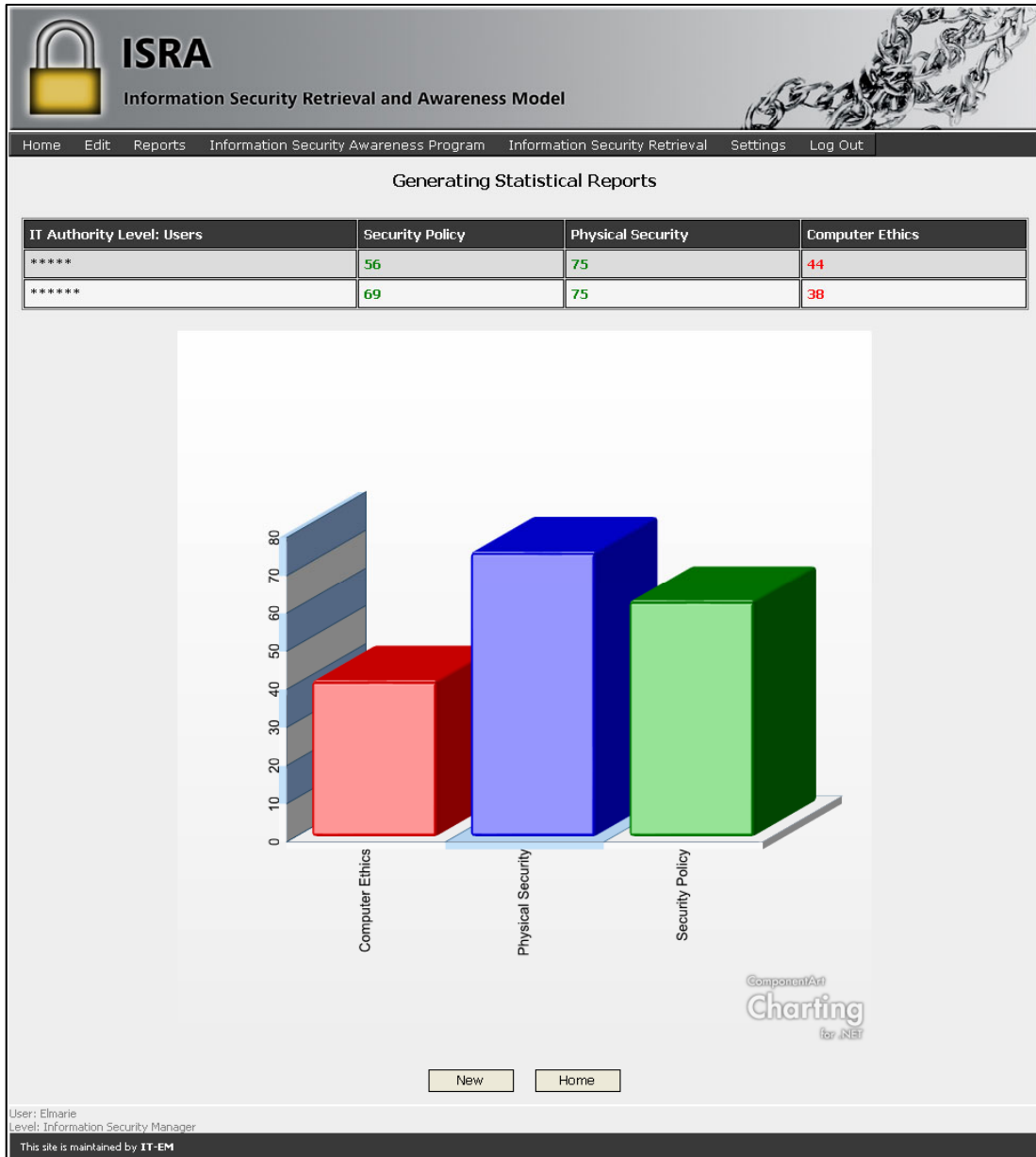
A list of Information Security issues (relevant to the IT authority level selected) will appear on the right-hand side of the screen (see Figure B58). Select one or more Information Security issue(s) on which the report should be based by clicking on the check box next to the appropriate Information Security issue(s). Click on the Home button to return to the home page (see Figure B6). Click on the Select button to generate the report as displayed on the screen depicted in Figure 58.



***Figure B58: Selecting an Information Security issue***

The results of the report will be displayed on the screen as depicted in Figure B59.





**Figure B59: Results of report**

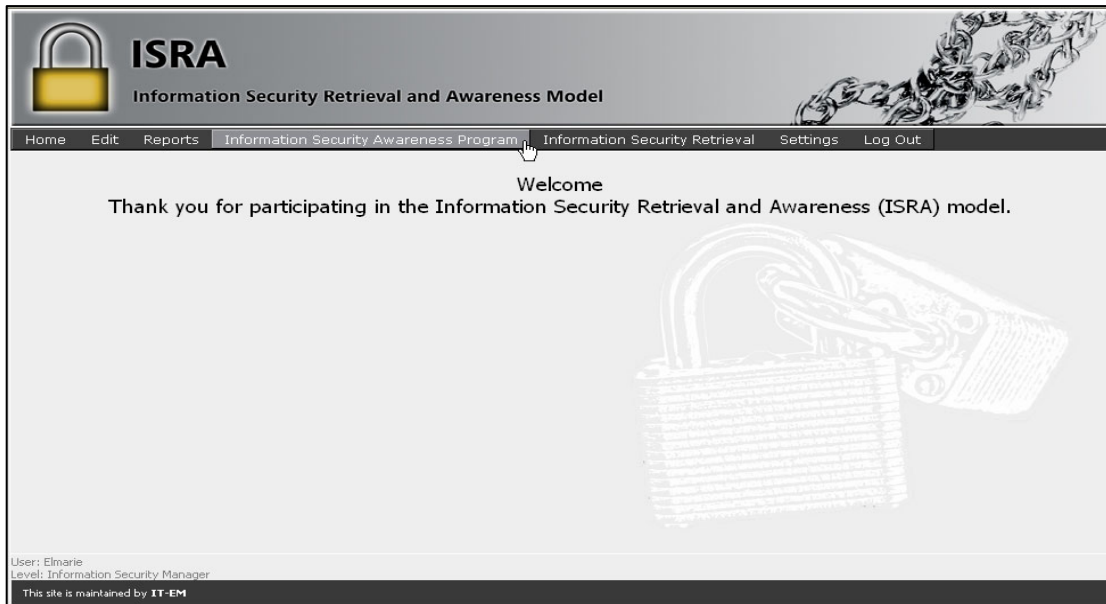
The results are displayed in a tabular as well as a graphical format. The tabular format displays the names<sup>1</sup> of the stakeholders on the requested IT authority level, together with their latest test results (0%-100%) for each relevant Information Security issue. All test results above 50% are indicated in green and those below 50% are indicated in red. The data presented in the table is also graphically displayed on a bar chart. The x-axis indicates the relevant Information Security issues, while the y-axis indicates the average percentages (0%-100%) achieved by all the stakeholders on that specific IT authority level, and for each relevant Information Security issue.

<sup>1</sup> The names of the stakeholders have been disguised to protect their identity.

To generate another report, click on the New button at the bottom of the screen. Alternatively, click on the Home button to return to the home page.

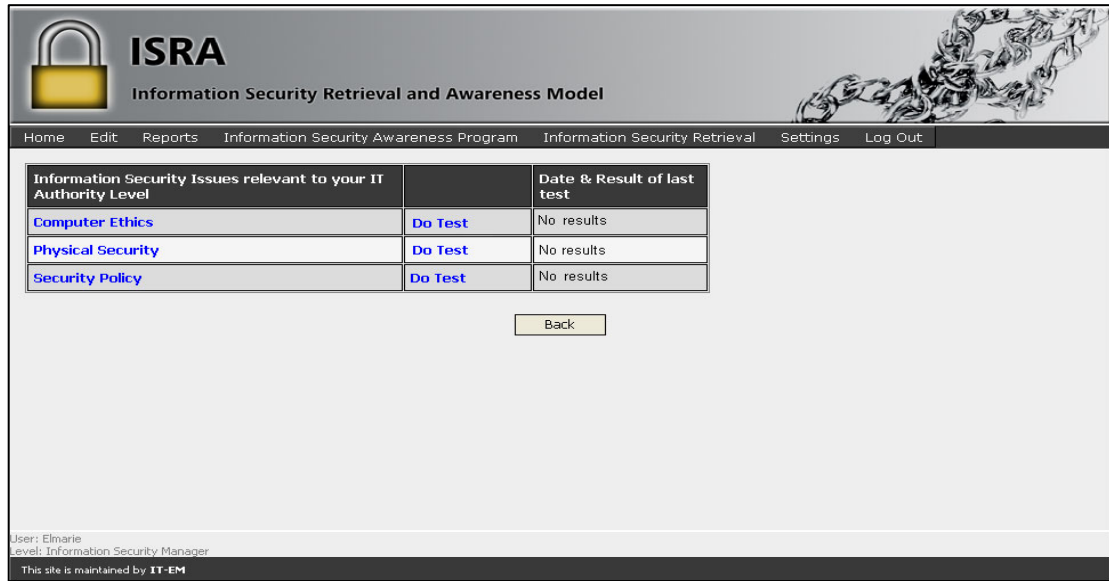
### B3.5 Information Security awareness program

If you want to participate in the Information Security awareness program, click on the Information Security Awareness Program option on the menu bar (see Figure B60).



*Figure B60: Information Security Program option*

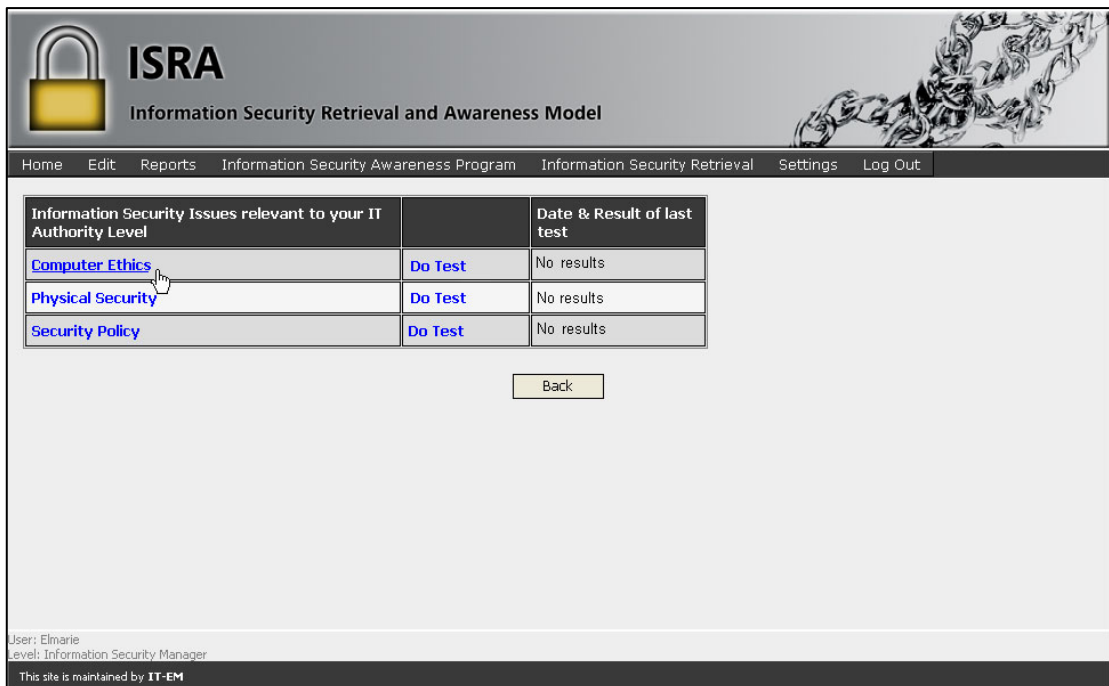
After you have clicked on the Information Security Awareness Program option, the Information Security issues relevant to your IT authority level (currently stored in the database) will be displayed in a table format (see Figure B61).



**Figure B61: Information Security issues related to IT authority level**

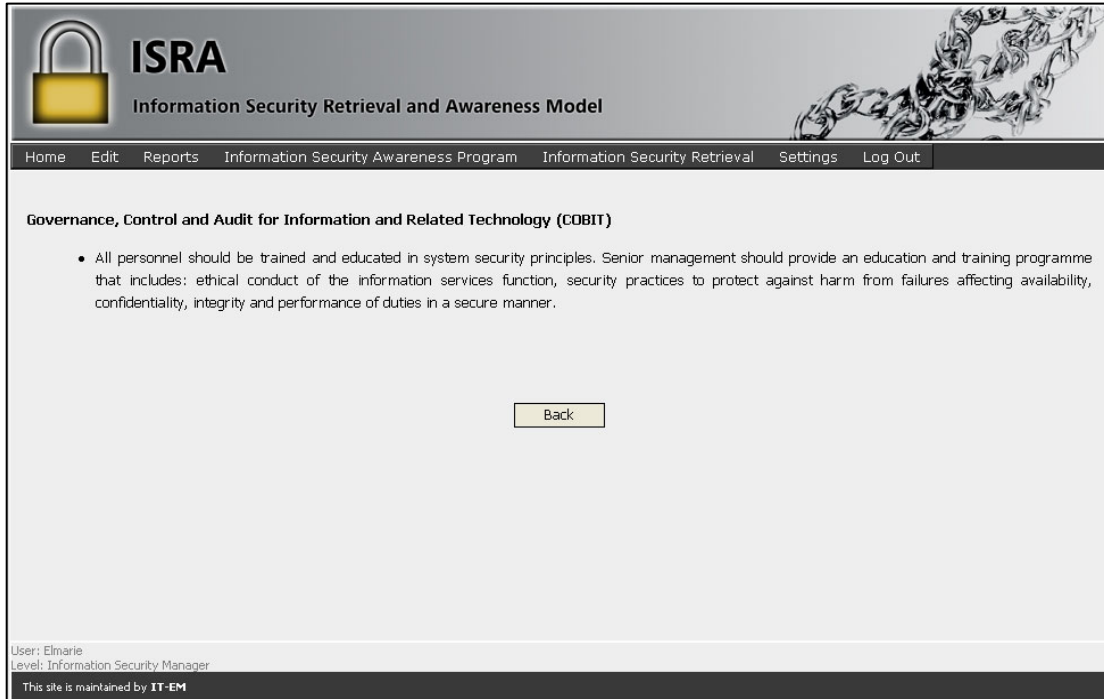
The table provides links to retrieve more information on each Information Security issue, as well as links to complete the Information Security test for each issue. The date and results of the last test that was completed are also listed in the table.

To retrieve detailed information regarding an Information Security issue, click on the specific Information Security issue as indicated in Figure B62.



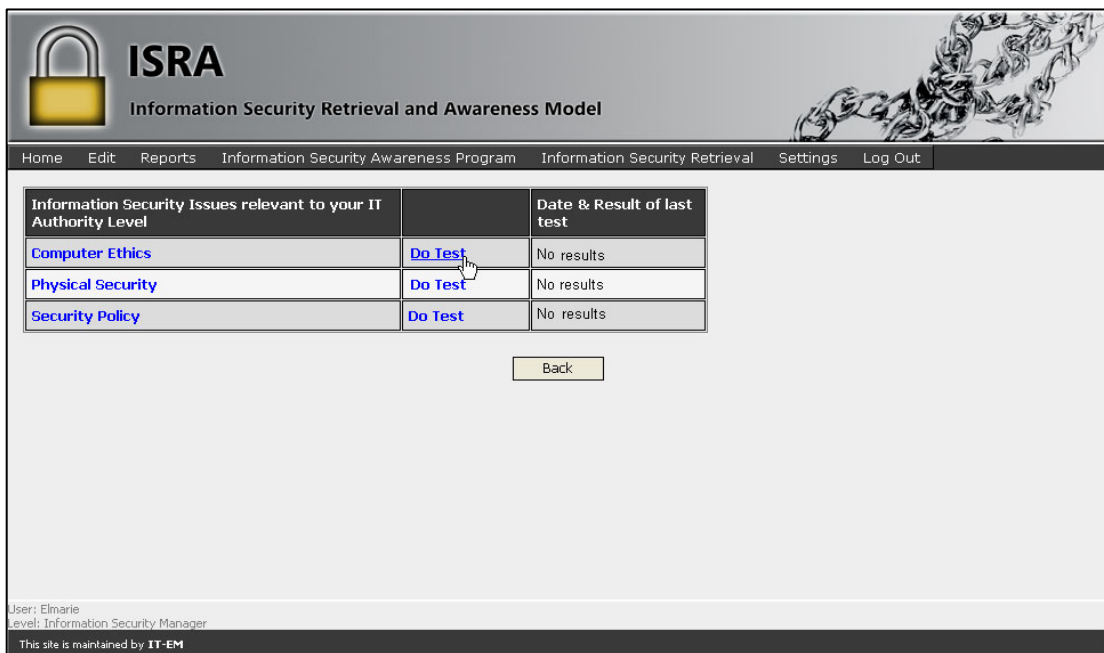
**Figure B62: Select computer ethics for more information**

You will be presented with information on the selected Information Security issue relevant to your IT authority level as is depicted in Figure B63.



**Figure B63: More information on computer ethics**


Click on the **Back** button to return to the previous screen (Figure B62). If you want to complete (or redo) the test for a specific Information Security issue, click on the **Do Test** link next to the appropriate Information Security issue, as indicated in Figure B64.



**Figure B64: Select to complete computer ethics test**


You will be presented with multiple choice questions pertaining to the selected Information Security issue. The number of questions for each test is specified by the Information Security Manager (see paragraph B.3.7.2) for each Information Security issue.

Select the correct answer for each question by clicking on the radio button next to the correct answer. If you have clicked on a radio button and want to change your answer, simply click on the alternative radio button. If you do not want to submit your answers, click on the `Cancel` button at the bottom of the screen. Alternatively, if you have answered all the questions, click on the `Submit` button as depicted in Figure B65.



## ISRA

Information Security Retrieval and Awareness Model



[Home](#)
[Information Security Awareness Program](#)
[Information Security Retrieval](#)
[Log Out](#)

Please complete the assessment questions for Computer Ethics

- 1) Ethics is a situational issue.

True

False
- 2) Copyright is an ethical issue.

False

True
- 3) There is \_\_\_\_\_ relationship between ethics and computer ethics

an indirect

no

direct
- 4) Ethics can be seen as a set of prescribed rules or a code of behaviour that is to determine between \_\_\_\_\_.

all computers

all stakeholders
- 5) Ethics is a set of \_\_\_\_\_.

rules set by law to determine what is right or wrong

principles based on religious rules and regulations

principles for justifying what is right or wrong
- 6) Ethics is about honesty, fair play, proper compensation and respect for privacy.

False

True
- 7) Ethical standards are \_\_\_\_\_ principles.

idealistic

legal

religious
- 8) Ethics is a complex issue.

True

False

9) Ethical standards are \_\_\_\_principles.

idealistic  
 legal  
 religious

10) Adhering to a Code of Ethics is to do what is right and to \_\_\_\_\_what is wrong.

report  
 disregard  
 ignore  
 disguise

11) It is unethical to download unauthorised software on your work computer.

False  
 True

12) Ethics should be part of the day-to-day activities of all employees.

True  
 False

13) Copyright is an ethical issue.

False  
 True

14) Ethics is about honesty, fair play, proper compensation and respect for privacy.

False  
 True

15) Ethics is described as \_\_\_\_\_.

legislatures representing all people  
 unwritten principles  
 a formal, written document

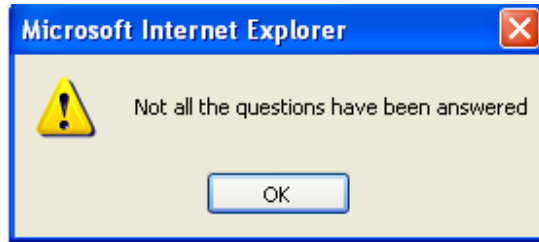
16) Ethical conduct may influence your professional status.

True  
 False

User: Elmarie  
 Level: Information Security Manager  
 This site is maintained by IT-EM

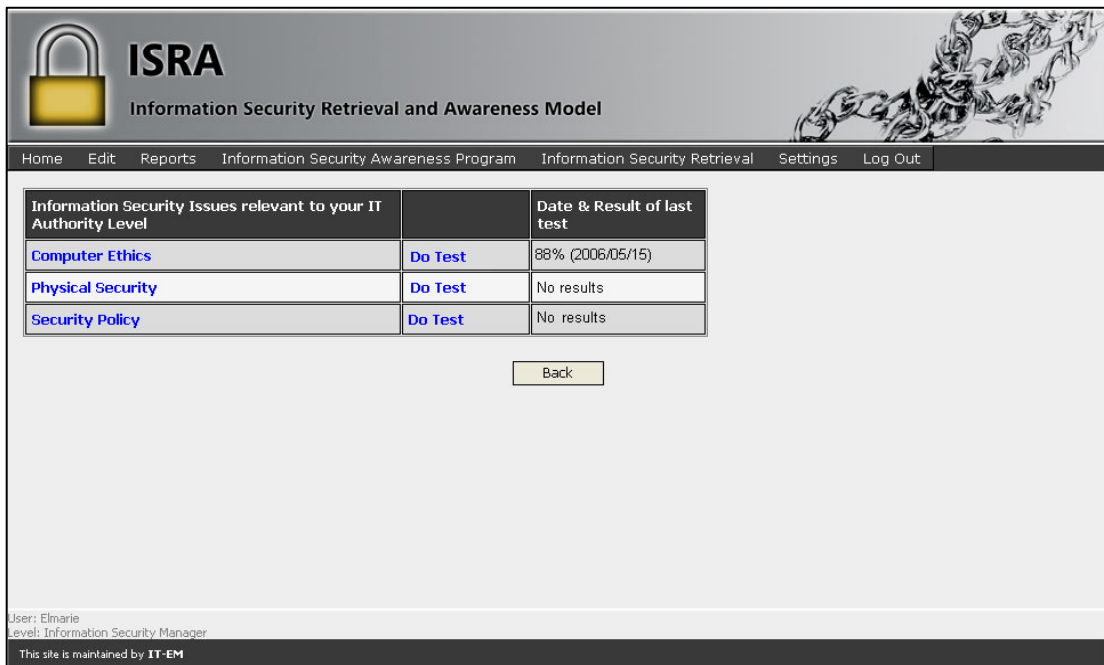
**Figure B65: Information Security awareness test on computer ethics**

If you have left out one or more of the answers, a warning that you have done so, will be displayed (see Figure B66). To proceed, click on the OK button, and fill in the missing answers.



*Figure B66: Warning to answer all questions*

After you have completed the test, the database will be updated, and your results and the date on which you completed this test will be displayed next to the relevant Information Security issue (see Figure B67).



*Figure B67: Results and date of the latest computer ethics test*

Click on the Back button to return to the Home screen.

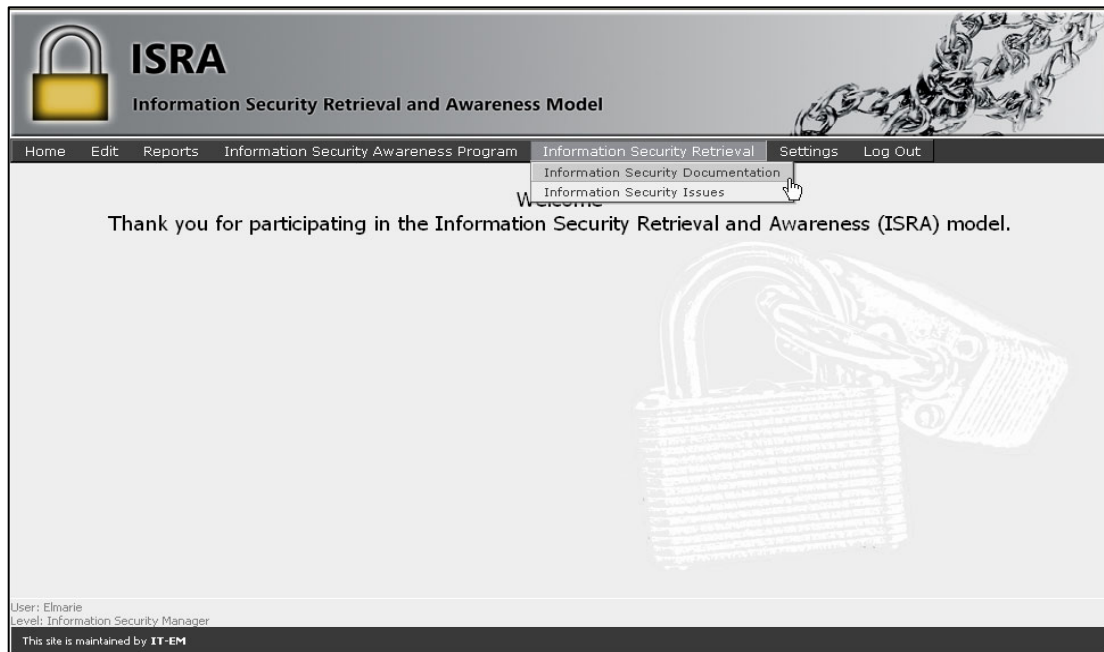
### **B3.6 Information Security Retrieval function**

There are two options to retrieve information from the database. The first option is by means of Information Security documents (see B.3.6.1) and the second option is by means of Information Security issues (see B3.6.2).



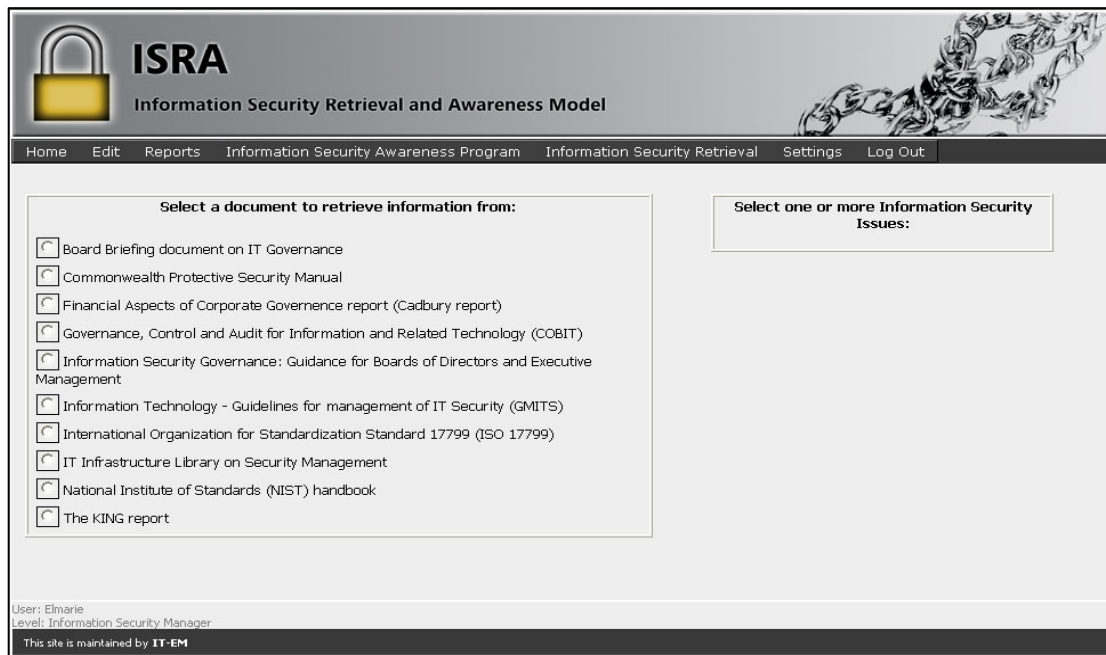
### B.3.6.1 Information Security documentation

If you want to retrieve information by using the Information Security documentation option, click on Information Security Documentation under the Information Security Retrieval option on the menu bar, as indicated in Figure B68.



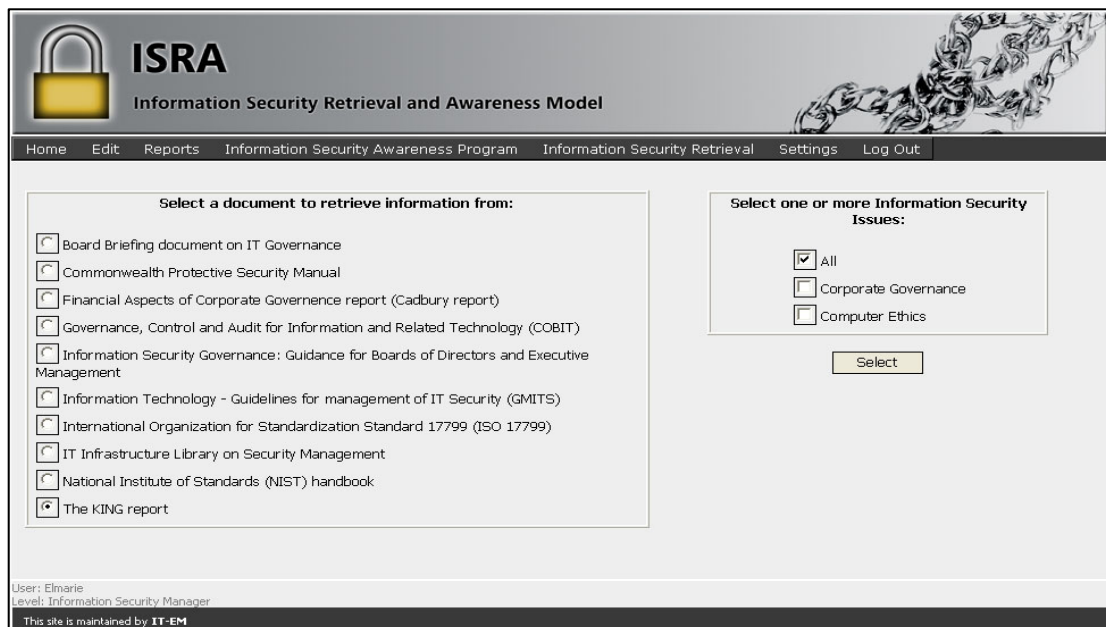
**Figure B68: Information Security documentation retrieval process**

After you have clicked on the Information Security Documentation option, the Information Security documents currently stored in the database are displayed (see Figure B69).



**Figure B69: Select relevant document**

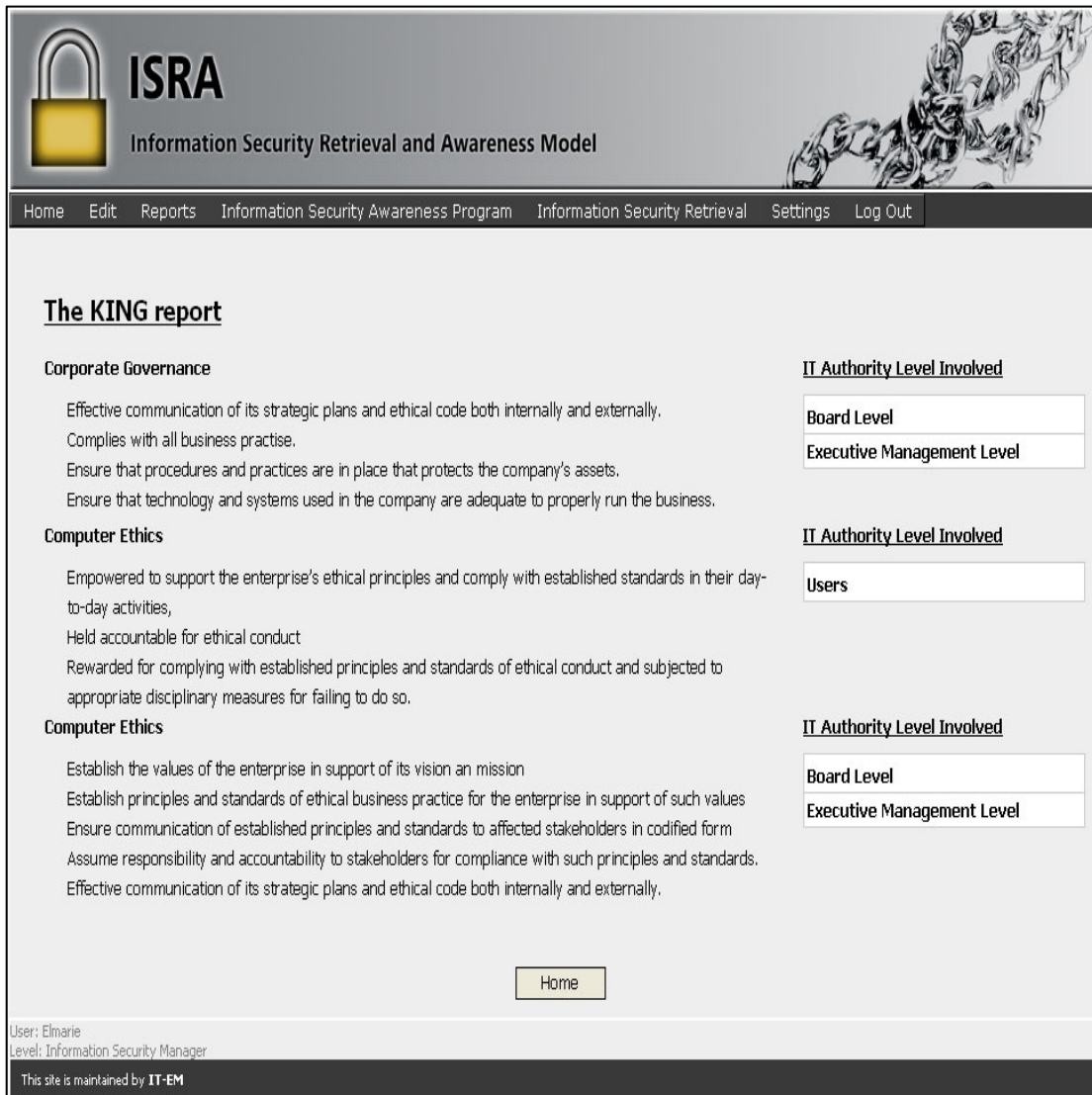
Select the relevant document from which you want to retrieve information by clicking the check box next to the appropriate document. A list of the Information Security issues related to the document that you chose will appear on the right-hand side of the screen. Select one or more of these Information Security issues by clicking on the check box next to the appropriate one(s) as shown in Figure B70.



**Figure B70: Select relevant Information Security issue(s)**

Click on the **Select** button.

The information on one or more Information Security issues that you have requested from a specific document, will be displayed on the screen – as depicted in Figure B71.



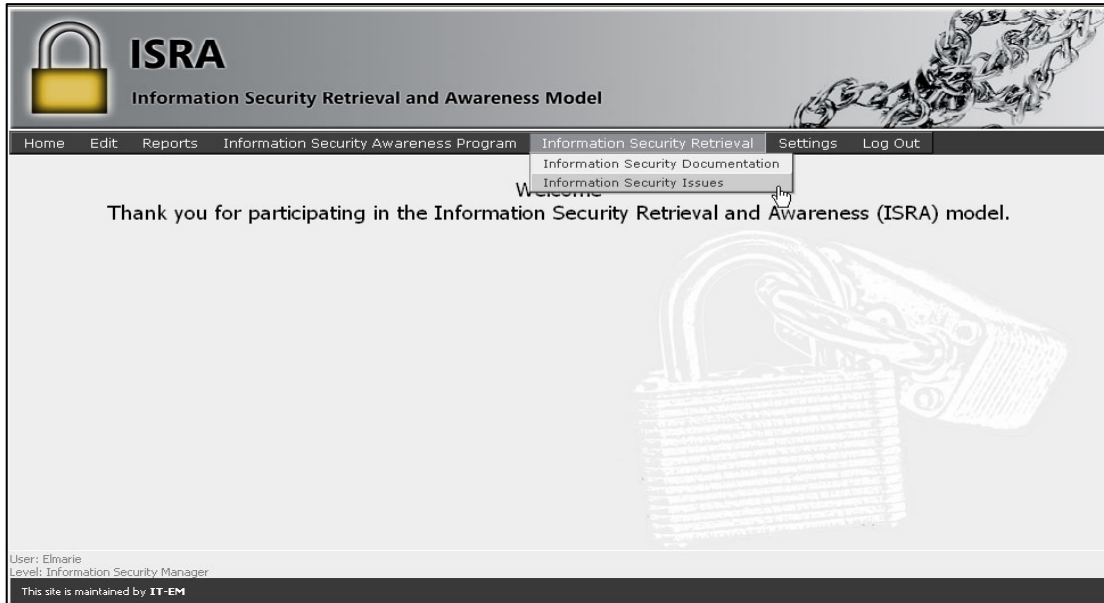
**Figure B71: Information obtained for retrieval process**

In this case, the results reveal what the King Report states about corporate governance and computer ethics. The results also include an indication of the IT authority level that should be aware of the information.

The Home button at the bottom of the screen will return you to the Home screen.

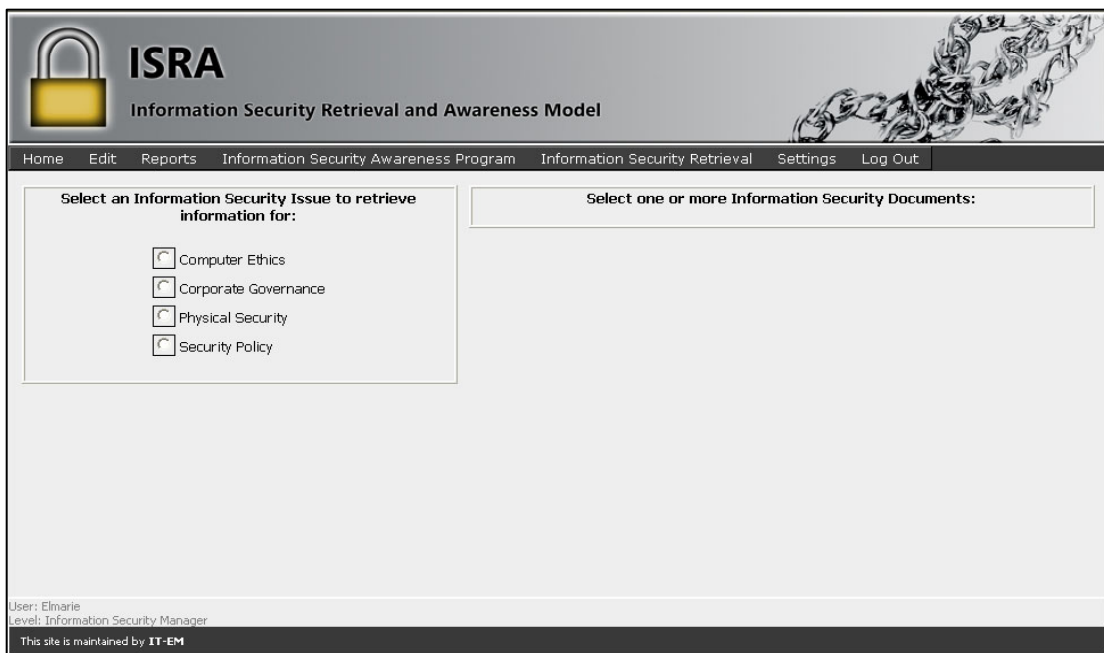
### B.3.6.2 Information Security issues

If you want to retrieve information by using the Information Security issues option, click on Information Security Issues under the Information Security Retrieval option on the menu bar, as indicated in Figure B72.



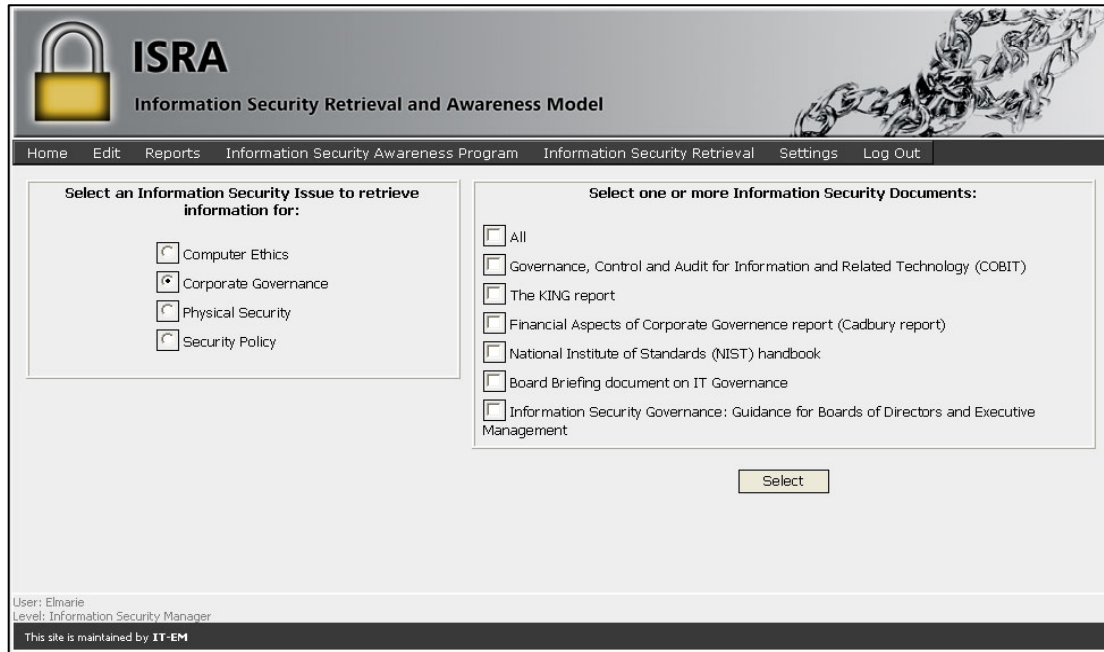
*Figure B72: Information Security issues retrieval*

After you have clicked on the Information Security Issues option, the Information Security issues currently stored in the database are displayed (see Figure B73).



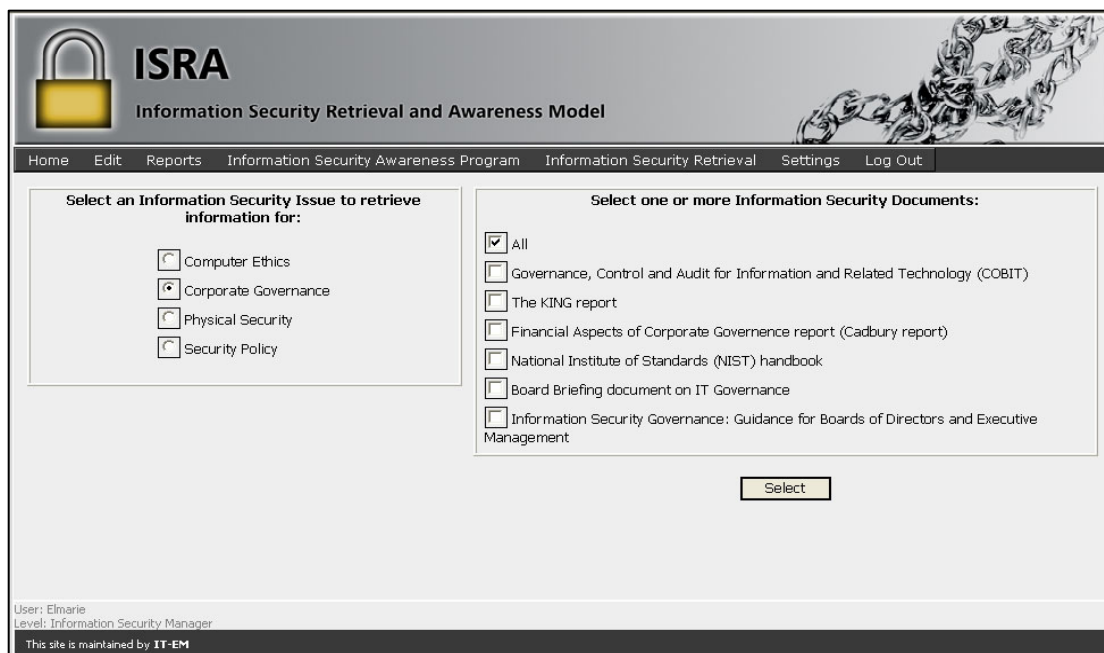
*Figure B73: Select relevant Information Security issue*

Select the relevant Information Security issue on which you want information by clicking on the radio button next to the appropriate Information Security issue. A list of documents containing information on the particular Information Security issue chosen in the previous step will appear on the right-hand side of the screen as depicted in Figure B74.



**Figure B74: List of relevant Information Security documents**

Select one or more of the documents by clicking on the check box next to the appropriate document as is indicated in the screen depicted in Figure B75.



**Figure B75: Select relevant Information Security document(s)**

Next click on the **Select** button. The information you have requested on the specific Information Security issue will then be displayed for each document that you requested (see Figure B76).

**ISRA**  
Information Security Retrieval and Awareness Model

Home Edit Reports Information Security Awareness Program Information Security Retrieval Settings Log Out

**Corporate Governance**

**Board Briefing document on IT Governance**  
Corporate Governance is to:

- Setting aims
- Providing the leadership to put them into effect
- Supervising the management of the business
- Report to shareholders
- IT resources to be used responsibly

**IT Authority Level Involved**

Board Level
Executive Management Level

**The KING report**  
Effective communication of its strategic plans and ethical code both internally and externally. Complies with all business practise. Ensure that procedures and practices are in place that protects the company's assets. Ensure that technology and systems used in the company are adequate to properly run the business.

**IT Authority Level Involved**

Board Level
Executive Management Level

**National Institute of Standards (NIST) handbook**  
According to NIST senior management has ultimate responsibility for the security of an organization's computer systems.

**IT Authority Level Involved**

Board Level
Executive Management Level

**Governance, Control and Audit for Information and Related Technology (COBIT)**  
Control which includes policies, organisational structures, practices and procedures, is management's responsibility. Management, through its **corporate governance**, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance or operation of information systems

**IT Authority Level Involved**

Board Level
Executive Management Level

**Information Security Governance: Guidance for Boards of Directors and Executive Management**  
For Information Security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required.

- Understand why information security needs to be governed
- Ensure it fits in the IT Governance framework
- Take Board level action
- Take Management Level action
- Information security policy
- Legal aspects
- Third party testing
- Employee awareness
- Adopt Best Practices

**IT Authority Level Involved**

Board Level
Executive Management Level

**Financial Aspects of Corporate Governance report (Cadbury report)**  
The agency head is responsible for ensuring that the agency has in place procedures for identifying information resources at risk and providing protection for them. Senior Management is responsible for, and should support, the implementation and maintenance of information security procedures within the areas under their control.

**IT Authority Level Involved**

Board Level
Executive Management Level

Home

User: Elmarie  
Level: Information Security Manager  
This site is maintained by IT-EM

**Figure B76: Information obtained for retrieval process**

In this case, the results reveal what all the documents in the database (as displayed in Figure B76) state about Corporate Governance. The results also include an indication of the specific IT authority level that should be aware of the information.

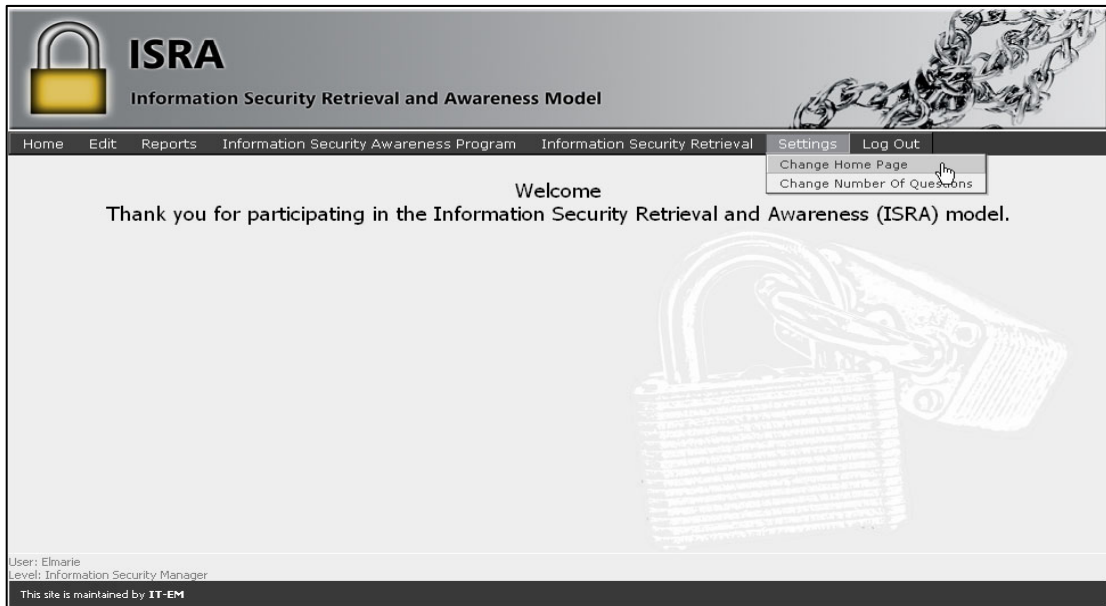
The **Home** button at the bottom of the screen will return you to the Home screen.

## B3.7 Settings

The Settings function has two options, the Change Home Page option (B3.7.1) and the Change Questions Count option (B3.7.2).

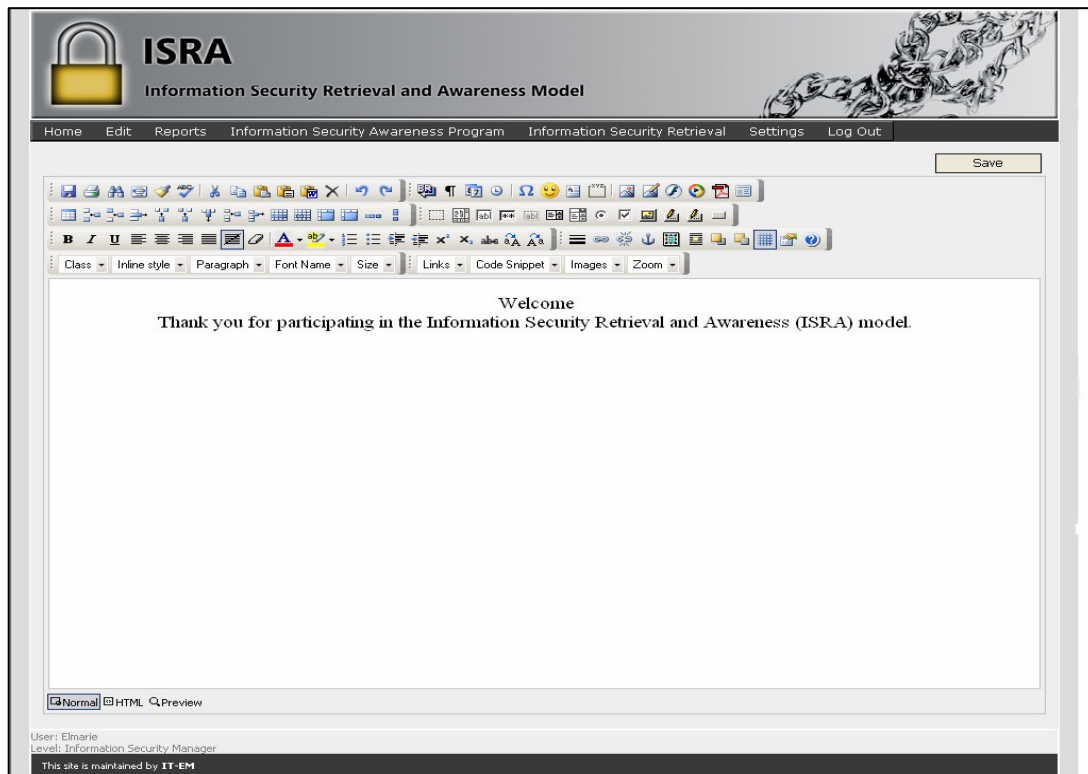
### A3.7.1 Change Home Page

If you want to change the home page, click on the Change Home Page option under Settings on the menu bar, as indicated in Figure B77.



**Figure B77: Change Home Page**

You will now be presented with the screen depicted in Figure B78.



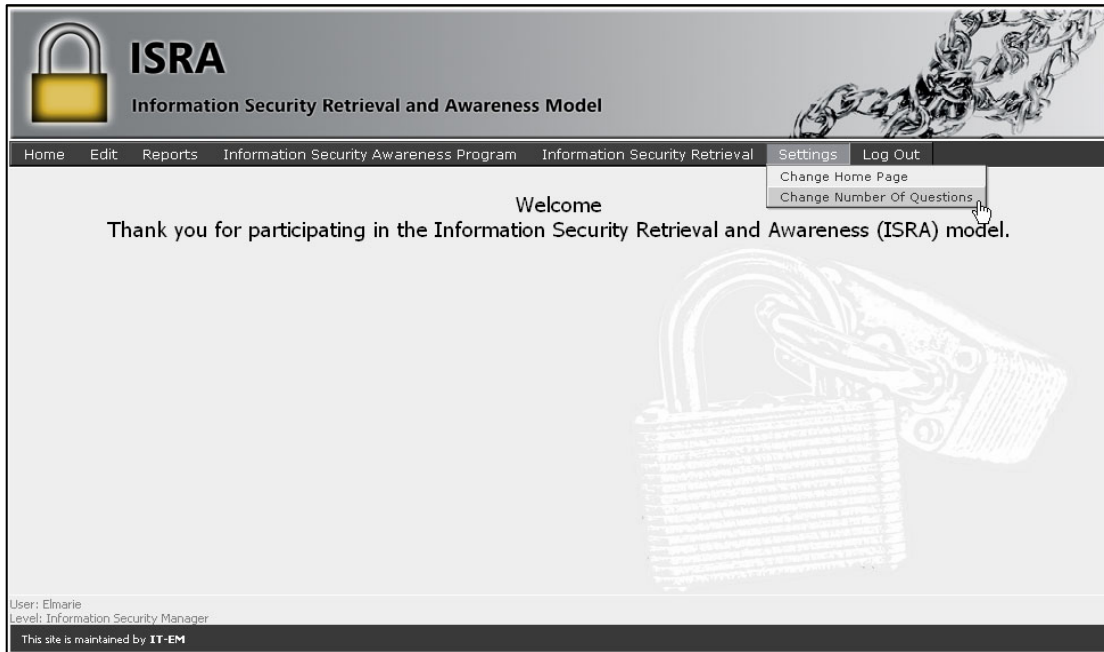
*Figure B78: Change Home Page*

Type in a new message or change the current message by using the toolbars. The function of each button on the toolbar is revealed when hovering the mouse over a specific button. After you have made the changes to the Home screen, click on the **Save** button to update the database. The new updated Home screen will be displayed.

### **B3.7.2 Change number of questions**

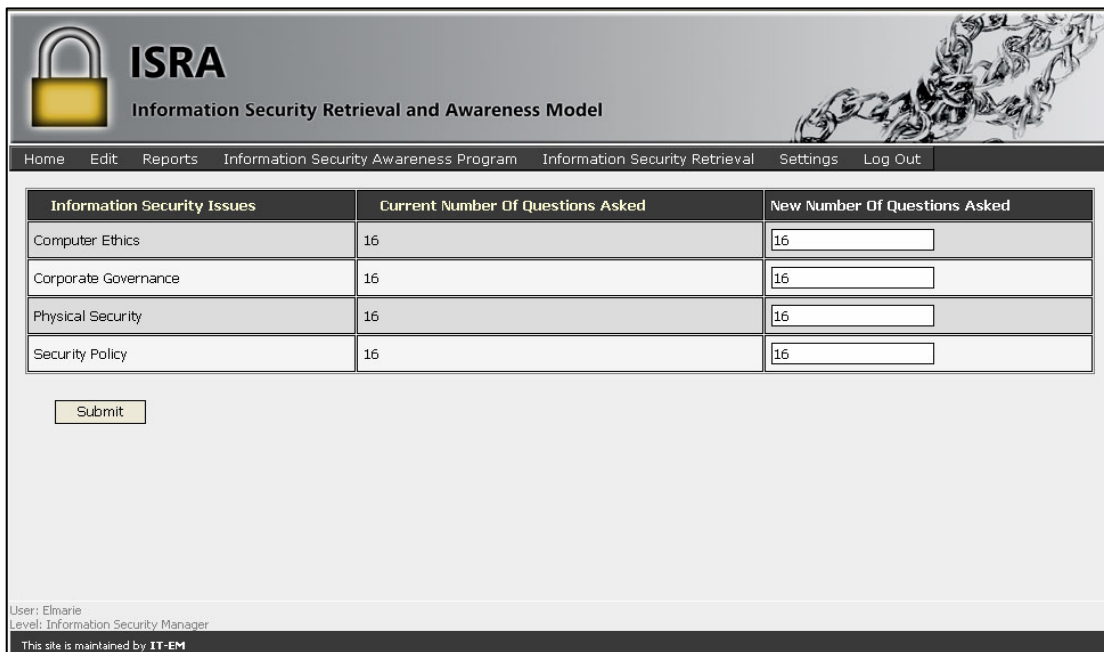
If you want to change the number of questions of the Information Security Awareness tests, click on the **Change Number of Questions** option under the **Settings** option on the menu bar, as indicated in Figure B79.





**Figure B79: Change number of questions option**

The screen depicted in B80 will be displayed as a result.



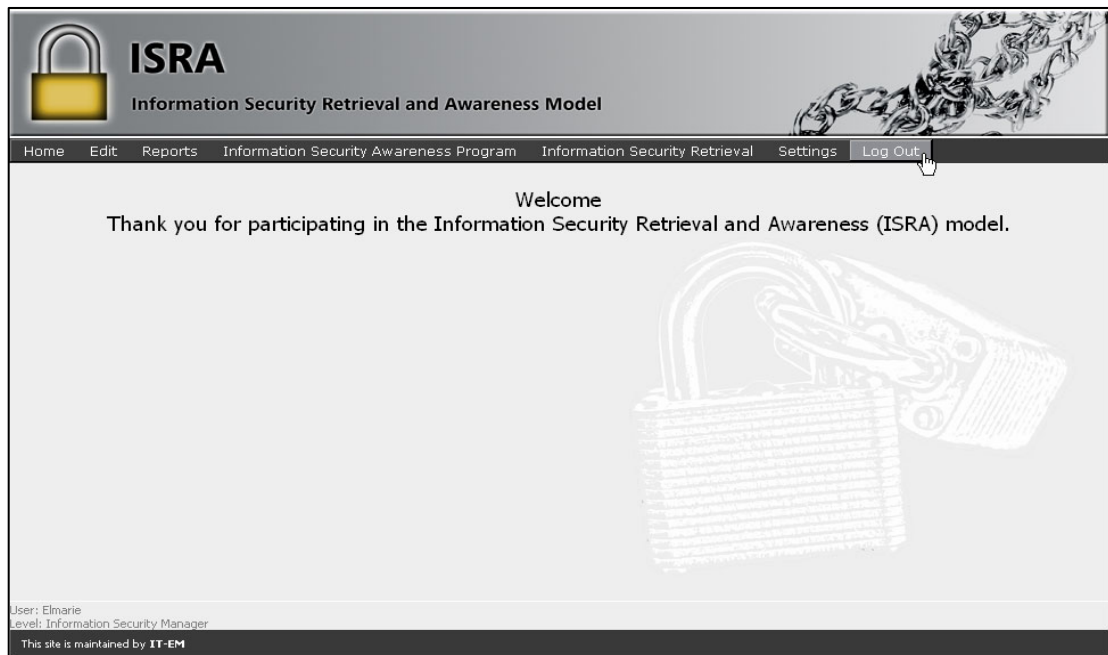
**Figure B80: Change number of questions**

This screen displays a list of all Information Security issues, with the number of questions currently asked on each Information Security issue. The last column can be edited to change the number of questions asked on a specific Information Security issue. To change this number, type a new number in the appropriate row in the last column, and

click on the `Submit` button. The database will now be updated to accommodate this change.

### B3.8 Logout

If you want to exit the program, click on the `Logout` option on the menu bar, as indicated in Figure B81.



*Figure B81: Log Out*

The initial login screen (depicted in B6) will be displayed as a result.

# **Appendix C**

**Paper presented at the Learning  
Conference, London UK, June 2003**

# Information Security Education in Non-Technical aspects of IT

*E. Kritzinger*

*Department of Computer Science and Information Systems*

*University of South Africa, Pretoria, SA*

*e-mail: [kritze@unisa.ac.za](mailto:kritze@unisa.ac.za)*

*S.H. von Solms*

*Department of Computer Science*

*Rand Afrikaans University, Johannesburg, SA*

*e-mail: [basie@rkw.rau.ac.za](mailto:basie@rkw.rau.ac.za)*

**Abstract:** This paper highlights the importance of information security awareness, education and training among employees in any organisation. The paper proposes a matrix that will incorporate all the different non-technical (human) aspects that is required in information security. This proposed matrix can be used as basis for the creating and designing of an information security syllabus.

**Key words:** information security education, information security awareness, information security training

## 1. Introduction

In a growing competitive industry many organisations are dependant on their resources for survival. These resources include hardware/software, labour, space, time, and many more. One resource that is usually left out is **information**. Organizations must realize and understand that information is an extremely valuable resource and must be secured accordingly. Information security (IS) has become a much-discussed subject all over the world in the last few years. This is because information security is no longer a luxury, but a necessity in all organisations. The purpose of information security is to ensure business continuity and to reduce business damage by preventing and minimising the impact of security incidents.

Information security can be divided into two categories, the technical and the non-technical aspects. The first category, technical aspects, is well known in the information security

field and a lot of research has been done. Examples of technical aspects include firewalls, encryption and network configurations.

This paper will mainly focus on the second category, the non-technical aspects. The reason is that although this category is also well known, not a lot of research has been done in this field. The non-technical aspects can also be seen as the human component of information security. This is important because according to Siponen [SIP00] the human component has been recognized to have a crucial role in information systems security, but the human issues have not received much attention. The NIST Handbook [NIS00] enforces this issue by stating that people are a crucial factor in ensuring the security of computer systems. The reason for this is because human actions account for a far greater degree of computer-related loss than all other sources combined. Therefore, information security must also be addressed as a human oriented issue. The only way to reduce information security risks is to make employees more information security aware. This awareness also means that employees must take responsibility for their actions when working with information.

Organizations must realize that before they can enforce employee responsibility, they have to ensure that all employees understand information security and what it entails. Employees must realize that they work with sensitive information and must be trained in how to secure that information. After employees understand the importance of information security, only then can they be held accountable if the integrity, availability and integrity is compromised. According to Wood [WOO95] even the best information security technological solution is doomed to fail if the people involved do not support it. The process of training and educating employees is usually done by well designed information security programmes. This information security programme must therefore include all aspects that have an influence in one way or another on information security.

To eliminate any confusion in terminology, the definitions for education, training and awareness are:

- Security **education** is more in-depth than security training and is targeted for security professionals and those whose jobs require expertise in security. [NIS00]
- The main aim of **training** is to teach people skills that will enable them to perform their jobs more securely. [NIS00]
- **Awareness** stimulates and motivates those being trained to care about security and to remind them of important security practices. [NIS00]

In this paper information security *guidance* will be used if referred to all three definitions: training, awareness and education.

## 2. Views on Information Security Guidance Programmes

When investigating non-technical, human aspects (in an industry based information security guidance programme) three angles must be included. These three angles can be formulated into three questions.

- What non-technical (human) information security aspects must be addressed?
- To whom do you want to present these aspects to?
- What is the content of the aspects that must be addressed?

Designing and creating a programme for the *awareness, training and education* of employees is not something new. There are many different views, models and designs on how this can and should be done. [THO98][THO99][SCH01][NIS00]. These models are usually implemented in industries and/or in broad overview in academic courses.

Research done by Schou [SCH01] addresses the first question of what is the different information security aspects that are needed for information security. This research can be seen as a one dimensional approach. His research syllabi are mainly aimed at an academic syllabus and not for implementation in industry. His syllabus provides a brief overview of different information security aspects that are important in industry. On an academic level; a one dimensional approach is acceptable for providing a broad overview to students.

Thomason [THO99] goes one step further and addresses the first and second questions in his research. He specifies which information security aspects are important and he also includes the role players to whom these aspects are important. He identified three IT levels; Top Management, IT personnel and End-Users. This indicates that his research syllabi can be implemented in industry and can be seen as a two dimensional approach.

Another two dimensional international accepted approach is the NIST SP500-172 Training Matrix [NIS89] which was designed to be implemented in industry. This document as well as the previous two documents incorporates technical as well as non-technical information security aspects. This can be a problem if this approach is intended for non-technical employees. The reason is that these employees do not have to understand technical aspects if it is not in their job description.

The authors are of the opinion that on industry level a two dimensional approach is not acceptable. The reason is that the content of the information security aspects is still not addressed. It is also essential to separate technical and non-technical aspects in a guidance programme. This is because technical aspects usually overpower the non-technical aspects that can leave information security vulnerable.

The main aim of this paper is to investigate and design a three dimensional approach to an information security guidance programme that can be implemented in industry. This design will focus primarily on the three questions (that can also be seen as three dimensions) of information security, and can be summarized as:

- Dimension 1: Components
- Dimension 2: People (IT authority levels)
- Dimension 3: Content

These three dimensions are not stand-alone units but *interact* with each other. The three dimensions can also be *integrated* to create a matrix that contains the non-technical, human aspects that are needed for a security information guidance programme. Each of these three dimensions will now be briefly looked at.

### **3. Dimension 1: Non-technical Influences on Information Security**

This dimension refers to the “types” of human oriented knowledge required in IT. The NIST handbook [NIS00] states that people are a crucial factor in ensuring the security of computer systems and valuable information resources. This is because human actions account for a far greater degree of computer-related loss than all other sources combined. Organizations that have implemented strong protection mechanisms and have educated their staff are in the best position to protect their information from unauthorised disclosure or modification. Different non-technical aspects that are included in this dimension are:

- 3.1 Ethics
- 3.2 Professionalism
- 3.3 Information Technology Culture
- 3.4 Information Security Culture
- 3.5 Social Culture
- 3.6 User Awareness
- 3.7 Information Security Management
- 3.8 Legal Aspects
- 3.9 Risk Management
- 3.10 Corporate Governance aspects

Many of the aspects such as “user awareness” have been around for a number of years and a great deal of research has already been done. But some other aspects, such as ethics and legal aspects only started to become important due to the development of new technologies. A brief overview will be given on each of the different aspects mentioned above.

#### **3.1 Ethics**

Information security ethics is probably one of the most recent additions in the information security management environment. Many papers have already been published on ethics in general, but information security ethics, in particular, did not have such a wide exposure.

#### **3.2 Professionalism**

Many times organisations rely on their employees to uphold the image of the organisation to ensure good relationships within the organisation as well as with clients, partners and investors. Therefore, organisations must ensure the professionalism of all the employees. Professionalism includes aspects such as competence, accountability, personal character and conduct and loyalty. Information Technology and specifically Information Security require a growing level of professionalism.

### **3.3 Information Technology Culture**

Information security has developed over the past few years under the influence of new technologies. The ever-changing technological environment means that what is considered to be state of the art today will be obsolete by tomorrow and so security must keep pace with these ongoing changes. Security must be considered as an integral part of the systems development life cycle process and must be dealt with in a proactive manner in order to be effective.

### **3.4 Information Security Culture**

In today's ever changing environment, organisations must try to create and sustain a healthy information security culture. The focus of an information security culture is the encouragement of the proper planning and management of all information security issues in the organisation. Especially if organisations are so dependency on their data, information systems and networks as they are today. Information security must become part of the day-to-day culture (operation) of employees.

### **3.5 Social Culture**

Organizations must realize that employees in the organisation will automatically form different social cultures. These social cultures must be recognized and understood to find the optimal method to enhance the information security aspects in the organisation. The organisations must also try to combine the different social cultures to form one universal social culture that is beneficial to the organisation.

### **3.6 User Awareness**

Information security awareness is a widely publicised and talked-about issue in the business environment. The reason for this is that information security awareness is mainly a human-related issue. It is important to realize that "human issues" are the main cause of security breaches. [LEW00] The only way to reduce information security risks in an organisation is to make employees more information security aware. This awareness also means that employees must take responsibility for their own actions in the workplace.

### **3.7 Information Security Management**

Information security management is an ongoing process to protect and ensure the availability, integrity and the confidentiality of information. Information security management is also about understanding the risks, threats and vulnerabilities in the organisation. To manage these risks, threats and vulnerabilities, information security management must be proactive and ongoing; especially where its design, development, implementation and procedural processes are concerned. [INF99]



### **3.8 Legal Aspects**

Before 1990, work in organisations was done in closed-system environments where everybody was trusted. This meant that few or no legal problems appeared because incidents like fraud and theft were minimal. This all changed when the idea of open environments was introduced. The main force behind this shift was due to of better network connections like the Internet.

### **3.9 Risk Management**

Risk is the likelihood of damage, loss or injury and can be found in any organisation. One way to reduce risk is through risk management. Risk management consists of taking steps and following procedures, which will reduce different risks in the organisation.

### **3.10 Corporate Governance Aspects**

Until early 1990, it was the responsibility of one specific person or department to maintain information security in the organisation. The responsibility of information security shifted from one person (or department) to the entire organisation. This responsibility of information security is being implemented at senior management level as well as at the level of all other employees in the organisation. The reason for implementing information security at the top level is that when senior management personnel take responsibility for it, the rest of the organisation will follow.

In the next part of the paper we will investigate the different IT authority levels (the second dimension) that can be found in an organisation.

## **4. Dimension 2: IT Authority Levels in an Organisation**

This dimension refers to the different IT “*role players*” in a company. Many companies have different IT authority levels. These levels will typically determine the responsibility and the access to information in the company. The different levels can also differ from one organisation to another. These authority levels that can be found in a typical organisation include:

- Board Level
- Executive Management Level
- Middle Management Level
- Technical Management Level
- Security Management Level
- User Level

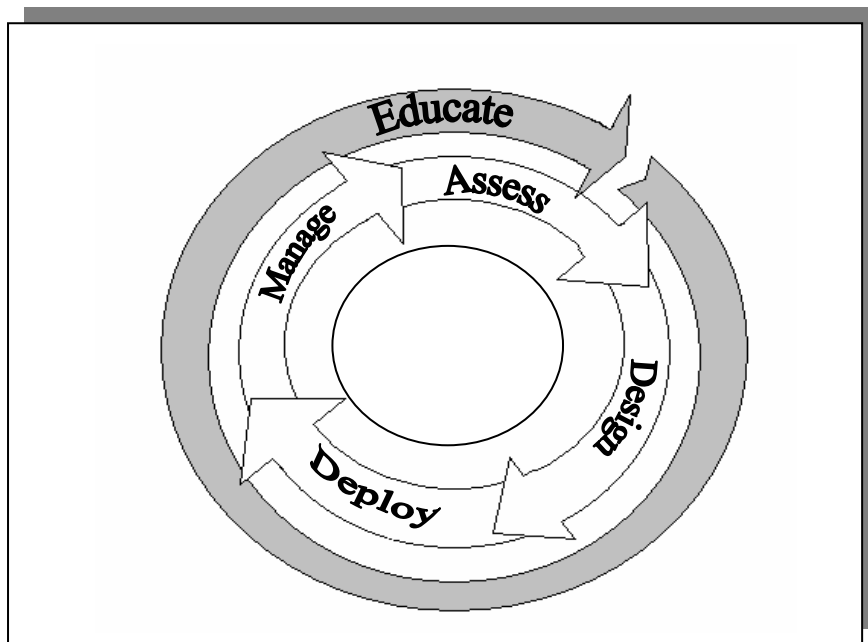
As already mentioned, each of these authority levels will have different knowledge requirements towards the information security in the organisation. For example, a user does not have to know or understand matters regarding the management of the organisation. So,

at the end, it is vital to indicate which authority level will be influenced by which non-technical aspects.

### 5. Dimension 3: Best Practices and Codes of Conduct

This dimension represents the interaction of different international documents such as Codes of conduct and Best Practices on which the first dimension will be based. That means that these Codes of Conduct and Best Practices will be used to determine which IT authority level (dimension 2) must include which non-technical aspects (dimension 1). Some of the Best Practices that are internationally accepted and will be used in the proposed matrix are COBIT, BSI-IT, ISO1 7799, and GMITS. Other documentation that will also be used is corporate government documents, documents of Professional Societies and legal documents. This dimension therefore identifies the knowledge base drivers for the first dimension.

The Internet Security Systems [ISS00] states that awareness can be obtained through employee education. This education is an ongoing effort to raise awareness of the need for information security at the senior management, administrator and end-user levels. The process cuts across all other security processes and can be depicted in the Figure 1 [ISS00]:

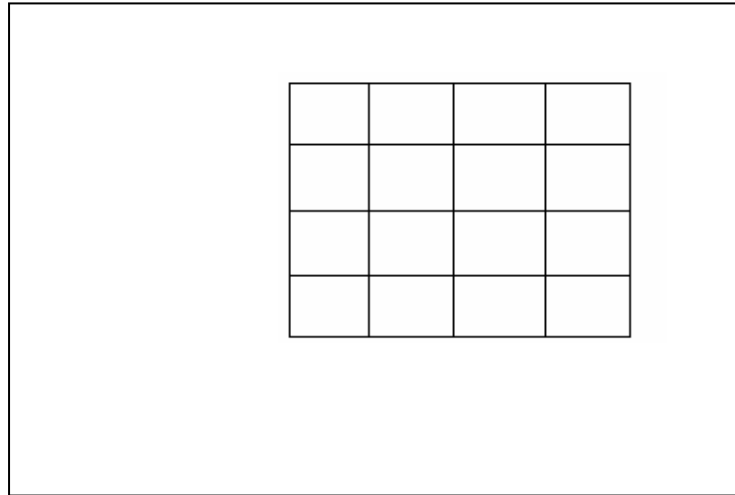


*Figure 1: Fundamental security management life cycle*

Figure 1 clearly shows that Best Practices and guidelines have a big influence on the management of information security education (awareness) in an organisation. The reason for this is that best practices and guidelines must form the basis of the information security guidance programme.

## 6. Three Dimensions

In this paragraph we will investigate the integration and interaction between the three dimensions. The first dimension (Components) is plotted on the y-axis while the second dimension (People) is plotted on the X-axis. The third dimension (Contents) is plotted as the different individual cells. This proposed framework of the matrix is depicted in Figure 2.



*Figure 2: Interaction of the three dimensions*

This interaction and integration can be seen as a multi-dimensional matrix that can be used as a basis to create an information guidance programme.

Each content document (as described earlier) is investigated individually to obtain the information relevant to the other two dimensions. The main aim of this matrix is to indicate two interacting relationships in this matrix. The first is which content document focuses on which information security component. That means which information security components (according to that document) are vital for information security.

For example, the King Report [KIN01] clearly states that corporate governance is very important in any organisation. The second relationship is to whom these information security components must be taught. In the example of the KING Report [KIN01] corporate governance (the components) must be handled by senior and executive management. Therefore, the King Report will be indicated in the cells corresponding to corporate governance and senior as well as executive management.

Another example is that the NIST document [NIS00] states that information security awareness must be included on all different IT authority levels. These examples (and some other examples) can be depicted in Figure 3.

Ethics						
Professionalism						
IT Culture						
IS Culture						
Social Culture						
IS Awareness	NIST	NIST	NIST	NIST	NIST	NIST
IS Management						
Legal Aspects						
Risk Management	King	King				
Corporate Governance	King NIST	King NIST				
	Board Level	Executive Management Level	Middle Management Level	Technical Management Level	Security Management Level	

**Figure 3: Three dimensions of the proposed matrix**

Please take note that the information in the figure is just an example to show the interaction of the three dimensions. These three dimensions will be expanded in more detail in further studies. This matrix will now be used to design a syllabus that can be implemented in industry.

## 7. Information Security Syllabi

The proposed syllabus will be designed according to the different relationships depicted in Figure 3. That means for each IT authority level a different information security guidance programme will be designed. Therefore each employee will be provided with information security guidance required for his/her IT authority level. Thus, a syllabus for senior and executive levels will only include information security components relevant to their IT

authority level. These information security components may be unique to some IT levels or some aspects may be found on all levels. Some other aspects that can differ between the syllabi are aspects such as presentation time, presentation method and testing methods. Each IT authority level will, as a result, have their own designed information security guidance programme. This programme will only contain the non-technical aspects that can be presented to employees with non-technical job descriptions.

## 8. Conclusion

There is no doubt that information is vital for the success of any organisation. Information must therefore be protected against all kinds of threats, whether by man or nature, whether intentional or accidental. One way to reduce threats by employees is through a well-designed information security guidance programme. That means employees must first be made aware, be trained and be educated about all information security aspects before they can be held accountable for their actions.

In the paper three non-technical information security dimensions were investigated. The interaction and integration between these three dimensions were depicted in a matrix. This matrix can then be used as a framework to design a multidimensional guidance programme. This guidance programme will contain only non-technical, human aspects that can be presented to non-technical employees. The programme is also divided in to sub syllabi for each individual IT authority level.

## 9. References

- [INF99] Information Systems Audit and Control Association, 1999: "*Information Security Policy.*" Online: [www.isaca.org.za](http://www.isaca.org.za)
- [ISS00] Internet Security Systems, 2000: "*Creating, implementing and managing the information security lifecycle.*" Online: <http://documents.iss.net/whitepapers/securityCycle.pdf>
- [KIN01] King Report, 2001: *The Code of Corporate Practices and Conduct*, (King Report), Institute of Directors, South Africa, version July 2001.
- [LEW00] Lewis A., 2000: "*Time to elevate IT security to the boardroom.*" E-secure, August 2000, Vol 1, Issue 1.
- [NIS89] NIST- National Institute of Standards and Technology, 1989: "*Computer Security Training Guidelines.*" Also available online: [www.nist.gov/](http://www.nist.gov/)
- [NIS00] NIST - National Institute of Standards and Technology, 2000: "*An Introduction to Computer Security*", The NIST Handbook." Also available online: [www.nist.gov/](http://www.nist.gov/)
- [PFL97] Pfleeger C.P., 1997: "*Security in Computing.*" Prentice Hall.
- [SCH01] Schou C.D., 2001: "*Information Security: International Curriculum Project*", Proceedings of the IFIP WG 11.8 Second World Conference on Information Security Education. Perth, Australia.
- [SEI00] Seifried K., 2000: "Ethics in Information Security." SecurityPortal Feb 25, 2001. Online: [www.securityportal.com/closet/closet200000531](http://www.securityportal.com/closet/closet200000531)
- [THO98] Thomson M.E. and Von Solms R., 1998: "*Information Security Awareness: Educating you users effectively*" Information Management & Computer Security, Volume 6, Issue 4, pp 167-173.
- [THO99] Thomson M., 1998: "*Make information security awareness and training more effective.*" Proceedings of the IFIP, TC 11.8, First World Conference on Information Security Education, Kista, Sweden, pp 261-270.

- [VON00] Von Solms S.H., 2000: "Information Security - The third wave?" Computer and Security, Volume 19 Issue 7, pp 615-620.
- [VON01] Von Solms S.H., 2001: "Information Security - A Multidimensional Discipline" Computer and Security, Volume 20 Issue 6, pp 504-508.

## **Appendix D**

**Paper published in the conference  
proceedings of the 10<sup>th</sup> International  
Conference on Information Systems  
Analysis and Synthesis, June 2004**

# **The NOKIS Model – A Model for Non-Technical Aspects of Information Security**

E. Kritzinger  
School of Computing  
University of South Africa, Pretoria, SA  
e-mail: [kritze@unisa.ac.za](mailto:kritze@unisa.ac.za)

and

S.H. von Solms  
Rand Afrikaans University, Johannesburg, SA  
e-mail: [basie@rau.ac.za](mailto:basie@rau.ac.za)

## **ABSTRACT**

This paper proposes a model that will incorporate all the different non-technical (human) aspects that are required in information security. The proposed model consists of three dimensions that are illustrated in a multidimensional matrix. The three dimensions of this matrix include information security components, people and documentation. The matrix will be used as a basis for creating and designing an information security syllabus to enhance information security awareness.

**Key words:** information security, non-technical aspects and information security model

## **1. INTRODUCTION**

According to Palmer [6], in recent years organizations have faced the challenge of a major computing paradigm shift. This shift was from proprietary networks and systems architectures to ‘open’ systems with distributed, heterogeneous servers and clients.

In this paradigm shift three development waves (stages) can be identified in the Information Security (IS) environment [11]. These three waves represent the development of IS from the middle 1950s. These three waves include:

- the technical wave (the first wave)
- the management wave (the second wave)
- the institutional wave (the third wave).

Figure 1 depicts the three waves as well as a timeline from the early 1950s to represent the different development stages in IS.



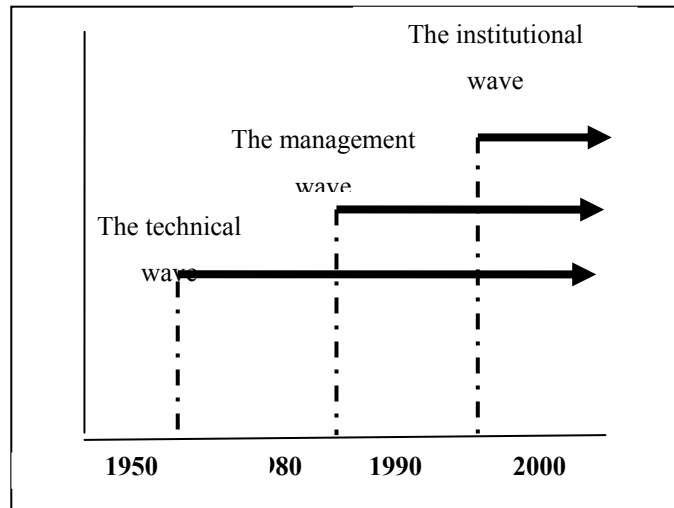


Figure 1: The different development waves [12]

It is important take into account that when the third wave started it did not replace the second wave, just as the second wave did not replace the first wave. [11] Although these waves are independent of one another, they still have an influence on each other. This is because the same issues can be found in different development waves. For example, an IS policy is found in both the management wave as well as the institutional wave. The difference is that in the management wave, for example, the main issue was the development of an IS policy. The institutional wave, however, is about the implementation and management of the IS policy. This means that a new wave improves the functionality of an existing wave. These three waves define the **Body of Knowledge (BOKIS)** that is required for the proper implementation of **IS**.

This body of knowledge for IS (BOKIS) includes all aspects and issues that have a direct as well as an indirect influence on IS. The BOKIS also includes all actions such as development, management and evaluation of IS aspects and issues. This BOKIS can be divided into two subsections – *technical* and *non-technical* aspects. This concept is depicted in Figure 2.

The first subsection focuses mainly on the technically oriented knowledge that is required to secure and protect information. The technical aspects include issues such as firewalls and encryption. These aspects are technical in origin and are usually only confined to the technical departments and employees in organizations.

The second subsection includes all the non-technical-oriented knowledge that is required to secure and protect information. It includes aspects such as ethics, legal issues and awareness. This second subsection can also be seen as part of the management side of securing and protecting information. The focal area of the second subsection is the different influences humans can have on information. These human influences can be classified as intentional or accidental and can be from outside as well as inside an organization. According to Lewis [3], IS is not so much a technical issue as a business issue.

The technical side of IS has been around far longer than the non-technical side due to the early origin of the technical wave. Figure 2 depicts that the first wave primarily contributed to the technical aspects of the BOKIS. Note that the second and third waves have also contributed to the technical aspects, but as a secondary contributor. The first wave has also had an influence, on a smaller scale, on the non-technical aspects. The second and third wave mainly contributes to the non-technical side of the BOKIS and form the basis for the NOKIS model – the non-technical-oriented (body of) knowledge for IS.

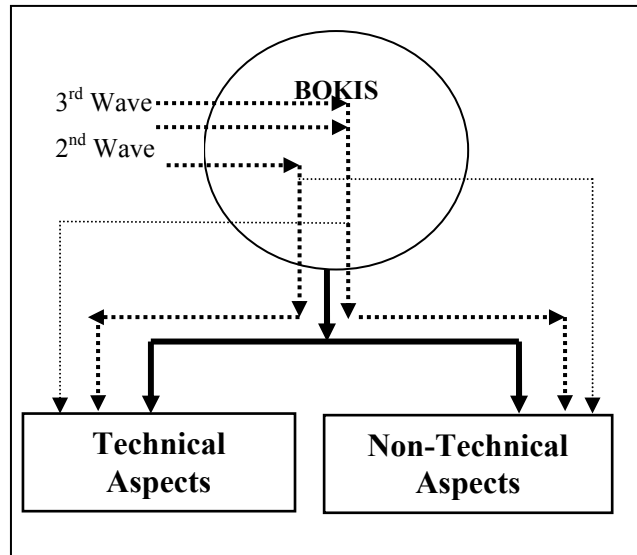


Figure 2: BOKIS

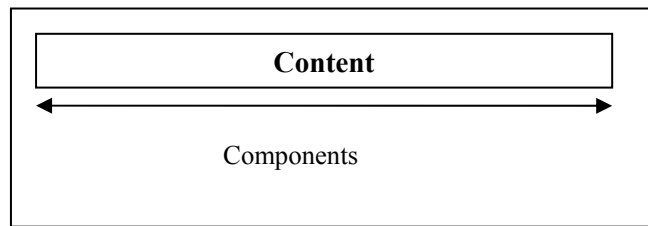
## 2. THE IMPORTANCE OF NON- TECHNICAL ASPECTS OF IS

The NOKIS model introduced in this paper will mainly focus on the non-technical aspects of the BOKIS. The reason for this is that in the IS environment, the technical side is far more established than the non-technical side. This is substantiated by Wright [13], who states that specialized attention is given to technical details, but little is taught about business security issues (e.g. risk management).

According to Siponen [8], the human component has been recognized as having a crucial role in information systems security, but the human issues have not received much attention. The NIST Handbook [4] reinforces this view by stating that people are a crucial factor in ensuring the security of computer systems. The reason for this is that human actions account for a far greater degree of computer-related loss than all the other sources combined. Therefore it is vital to draw a clear distinction between technical and non-technical aspects to ensure that technical aspects do not overshadow the non-technical ones. It is also essential to advocate that more research be done on the non-technical IS aspects in order to ensure that there is an equal balance between the technical and non-technical aspects. Due to the traditional under-emphasis on non-technical research and implementations, this paper will focus on the NOKIS model

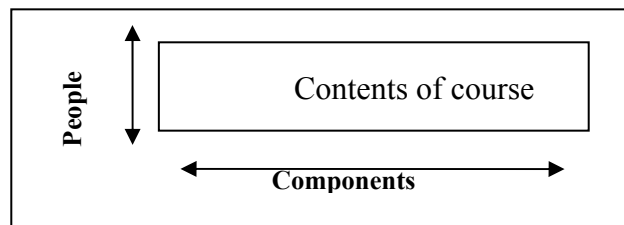
## 3. THE MULTI-DIMENSIONAL APPROACH

Research done by Schou [7] addresses the different IS components that are required to secure information. This research can be seen as a *one-dimensional* approach because these components do not distinguish between different people exposed to the content of the components. His research syllabi are mainly aimed at an academic application and not for implementation in industry. He provides a brief overview of different information security aspects that are important in industry. On an academic level a one-dimensional approach is acceptable for providing students with a broad overview. This one-dimensional approach is depicted in Figure 3.



*Figure 3: The one-dimensional approach*

Thomason [10] goes one step further and addresses a second aspect that is relevant to IS. This aspect includes all the different people that are involved in IS. Thomason specifies which IS aspects are important and he also includes the role players to whom these aspects are important. He identifies three IT levels: Top Management, IT personnel and End-Users. He therefore does distinguish between different (types) people to be exposed to the content. This indicates that Thomason's research can be seen as a *two-dimensional* approach. Figure 4 depicts this two-dimensional approach with the people on the y-axis and the components on the x-axis.



*Figure 4: The two-dimensional approach*

Another two-dimensional, internationally accepted approach is the NIST SP500-172 Training Matrix [5] which was designed to be implemented in industry. This document, as well as the previous two, incorporates technical as well as non-technical information security aspects. This can be a problem if this approach is intended for non-technical employees. The reason is that these employees do not have to understand technical aspects if they are not in their job description.

It is clear that there are many different views, models and designs on how this can and should be done [9][10][7][4]. However, the authors are of the opinion that a one or a two-dimensional approach is not rich enough due to the fact that different IS documentation, driving and specifying the content, is still not addressed. Therefore a three-dimensional approach is the next step. The following three aspects will be included in this three-dimensional approach:

- The different components comprising the Non-Technical-oriented body of knowledge needed to secure information.
- The different people (IT authority levels), depending on a company's hierarchy, to whom this body of knowledge must be imputed.
- The different national and internationally accepted Best Practices giving guidance on this body of knowledge.

Throughout the rest of this paper these aspects will be referred to as different dimensions in the IS environment. These three dimensions will form part of a multi-dimensional matrix. This matrix will form the underlying structure for the NOKIS model. **NOKIS** is an abbreviation for the Non-technical-Oriented Knowledge for Information Security that is required for IS. These three dimensions of the NOKIS matrix can be summarized as:

- Dimension 1: Components
- Dimension 2: People (IT authority levels)
- Dimension 3: Documentation (Best Practices).

Each of these three dimensions will now be briefly investigated to demonstrate the relationship in the multi-dimensional matrix.

### 3.1 Components

This dimension refers to the ‘types’ of human-oriented knowledge required in IT. Organizations which have implemented strong protection mechanisms and have educated their staff are in the best position to protect their information from unauthorised disclosure or modification. Different non-technical components which are included in this dimension are:

- Awareness
- Security Policy
- Senior Management (Corporate Governance)
- Legal aspects
- Ethics
- Logical Security
- Physical Security
- Information Classification
- Risk Management
- Information Security Management
- Training and Education
- Information Security Culture
- Best Practices Certification
- Personnel.

Some of these components have been around for a few years, for example the IS policy, whereas other aspects such as ethics and legal issues are fairly new. The different components mentioned above are only some of the components and issues that influence IS in one way or another. There are more, but for the purpose of this paper, a description of these aspects is enough to illustrate the concept of the NOKIS model. This dimension therefore specifies ‘what’ knowledge is needed.

### 3.2 People

This dimension refers to the different IT ‘*role players*’ in a company. Many companies have different IT authority levels. These levels will typically determine the responsibility and access to information in the company.

According to NIST [4] there are many different ways to identify individuals or groups who need specialized or advanced training. One method is to look at job categories, such as executive, functional, managerial or technological. Another method is to look at job functions, such as system design, system operation, or system use. A third method is to look at the specific technology and products used. This paper will use the first method to identify different IT authority levels that are important to IS. Each different authority level will have different components (information security aspects) that they are required to know, understand and to implement in their day-to-day environment.

These authority levels will differ from organization to organization, depending on their internal structure. The primary authority levels that can be found in a typical organization include:

- Board Level
- Executive Management Level
- Middle Management Level
- Technical Management Level
- Security Management Level
- User Level.

These are not the only IT authority levels in the IS environment, but are sufficient to illustrate the concept. Each of these levels can be further subdivided into more detailed IT authority levels. One example is the fact that NIST [4] divides the User level into two sublevels. The first sublevel consists of the users of information. These are individuals who use information provided by the computer. The second sublevel is comprised of users of systems. These are individuals who use the computer system directly. Many of the other IT authority levels can also be subdivided into different sublevels.

However, this paper will focus primarily on the main IT authority levels mentioned above. This dimension therefore specifies to ‘whom’ the knowledge is important.

### 3.3 Documentation

This dimension represents the interaction of different international documents such as Codes of conduct and Best Practices on which the first dimension will be based. This means that these Codes of Conduct and Best Practices will be used to determine which IT authority level (dimension 2) must include which non-technical aspects (dimension 1). This documentation is selected from a wide range of IT areas. These areas include:

- Best Practices
- Codes of Conduct
- Legal documents
- Corporate Governance documents
- IS Management documents
- Documents of Professional Societies.

Some of the documents that will be considered in for the NOKIS model include:

- COBIT
- BSI-IT
- ISO 7799
- GMITS (ISO/IEC TR 13335-1)
- King Report
- Guidance for Boards of Directors and Executive Management
- Board Briefing on IT Governance
- NIST - (IS Management document)
- Information Security Guidelines for NSW Government.

This dimension therefore specifies ‘where’ the relevant knowledge is to come from. These documents are not the only IS related documents but illustrate the concept of the NOKIS model.

## 4. THREE-DIMENSIONAL MATRIX

These three dimensions (as mentioned above) will form the cornerstones of the NOKIS matrix. The integration and interaction between the different dimensions will form the content of the NOKIS syllabi. The matrix and the syllabi together form the NOKIS model. This is depicted in Figure 5.

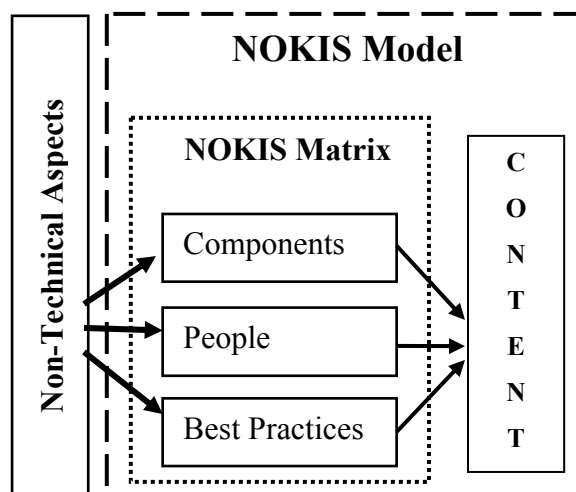
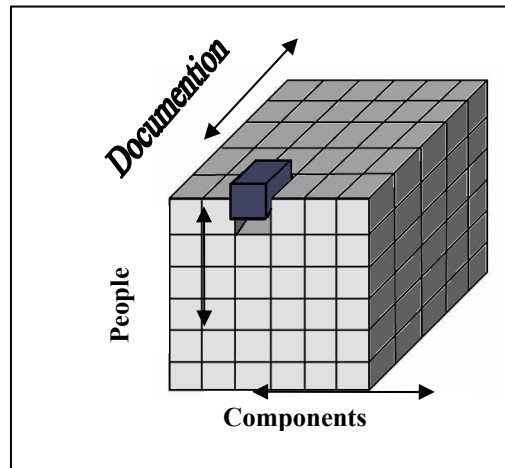


Figure 5: The NOKIS Model

In the rest of this paragraph we will mainly investigate the NOKIS matrix (depicted in the dotted line in Figure 5). This multi-dimensional matrix will consist of an **x**, **y** and **z** axis. The first dimension (Components –‘what’) is plotted on the **x** axis while the second dimension (People –‘who’) is plotted on the **y** axis. The third dimension (Documentation – ‘from where’) is plotted on the **z** axis. Each individual cell represents specific contents related to the three dimensions. This is depicted in Figure 6.



*Figure 6: The three-dimensional Matrix*

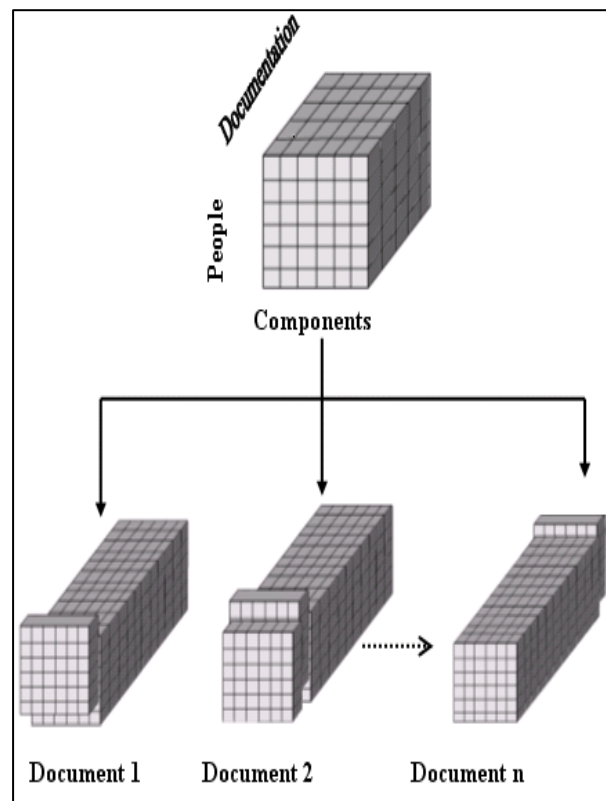
One advantage of a multi-dimensional matrix is that the information in the matrix can be viewed from different angles or viewpoints. These viewpoints can be primary viewed from the **x**, **y** or the **z** axis. Identifying a primary axis can be done by means of the slicing method. This slicing method can be seen as a tool to extract relevant information from the matrix.

The first angle that will be addressed is from the **z** axis (documentation). This viewpoint from the documentation side will show each document individually. This method is called **z**-slicing.

#### 4.1 Z-Slicing

The **z**-slicing method is used (in a multidimensional matrix) when information on different axes depends on the information from the **z**-axis. Therefore, the information on the **z**-axis will be the primary element and the information from the other axes will be the secondary elements. In the rest of this paragraph the third dimension (documentation) which is depicted on the **z**-axis will be used as the primary source.

Z-slicing extracts all relevant information regarding individual documentation in the matrix. Each z-slice will represent one document including the relevant information from the other two dimensions. Therefore, the z-slicing method will indicate, for each document, which IS components are important (relevant) on which IT authority level. This slicing method is depicted in Figure 7.



*Figure 7: Z-slicing*

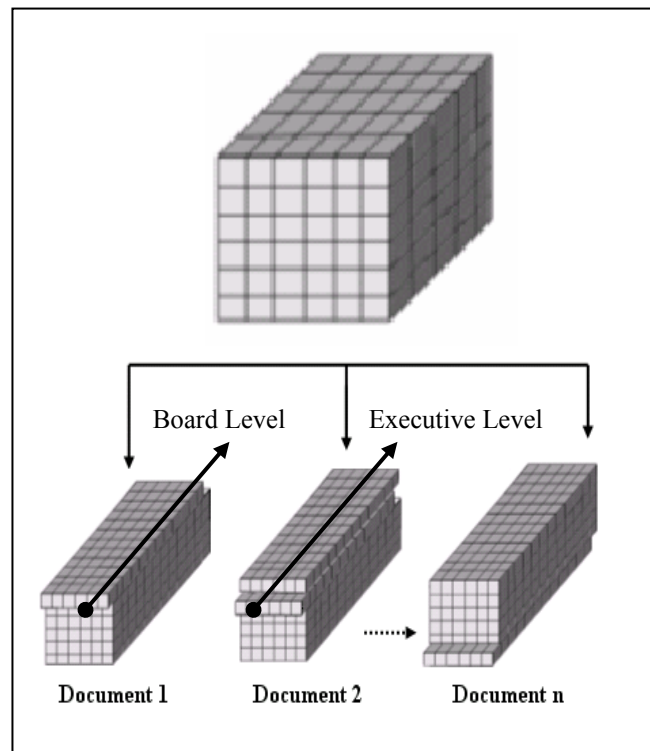
The information gathered from the use of this method will form the first part of designing the NOKIS syllabi. The second part of the syllabi can be gathered by using the y-slicing method.

Document 1 in Figure 7 therefore specifies the contribution ISO 17799 has made to the content of the NOKIS model for all the people concerned (role players) for all relevant components. In the same way Document 2 specifies the contribution COBIT has made for all the people concerned and all components.

#### 4.2 Y-Slicing

The y-slicing method will view the information in the matrix from the z axis. Y-slicing extracts all the information regarding individual IT Authority Levels. According to Irvine [1], it is unreasonable to suggest that everybody should know everything about security. She proposed matching appropriate knowledge and skills with typical roles in information society. The different roles in information society will mainly depend on the different authorisation levels to access information.

This matching of appropriate knowledge can be achieved by identifying the y axis (IT authority level) as the primary source. The information on the x and z axes are the secondary information. Therefore, the y-slicing method will indicate which IS components and obtain which documents are important (relevant) on which IT authority level. The y-slice method is depicted in Figure 8.



*Figure 8: Y-slicing*

The information collected from the use of this method can be further divided to obtain specific content for the NOKIS syllabi. This will be done by taking the results from the y-slice and slicing them again on the x-axis. Document 1 in Figure 8 therefore specifies knowledge required on Board Level specified over all contributing 'driver' documents for all relevant components. In the same way Document 2 specifies the knowledge required on Executive Management Level specified over all contributing 'driver' documents for all relevant components.

### 4.3 YX-Slicing

The yx-slicing method is done to extract the specific *content* from each cell in the matrix. Firstly a z-slice is taken (a specific IT authority level) and then sliced again in the x-axis (a specific IS component). This yx slice will indicate the specific IS component as well as the content (obtained from the documentation) that is relevant to that individual IT authority level. The result of this slicing method will be used as the building blocks for the NOKIS syllabi. This y x-slicing method is depicted in Figure 9.

If the xy-slicing is done, all the building blocks can be grouped together to design NOKIS syllabi. The main grouping will be done on the IT authority level. Therefore, each IT authority level will have its own IS syllabi which include all IS aspects that are relevant on their level. This will eliminate all unnecessary time, costs and effort expended on teaching employees IS issues that are not relevant to their IT authority level.



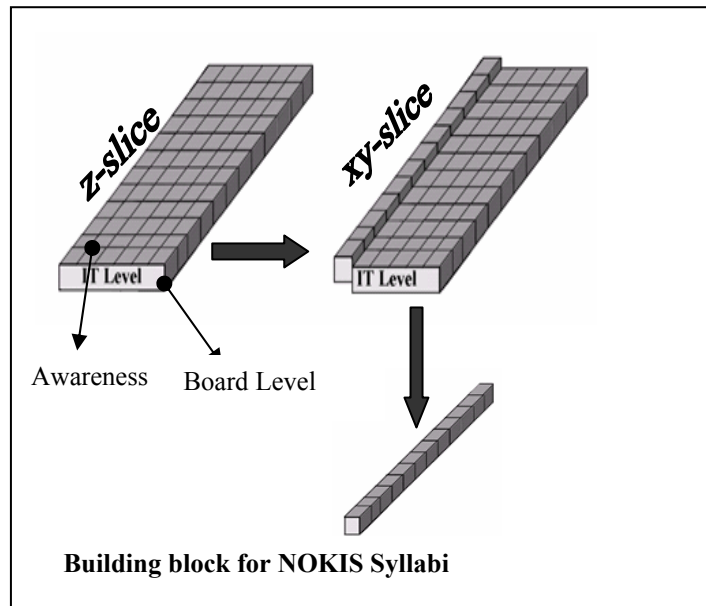


Figure 9: YX-slicing

The building block in Figure 9 therefore specifies the content, as defined by all relevant 'driver' documents for the syllabus of awareness courses on Board Level.

## 5. Conclusion

The NOKIS model is a multi-dimensional model that includes different components, people and best practices that is relevant in the IS environment. The NOKIS model can be used as the basis (or building blocks) to create and design a NOKIS syllabus. These syllabuses will contain only non-technical, human aspects that can be presented to non-technical employees. The programme is also divided into sub syllabi for each individual IT authority level.

## 6. References

- [1] Irvine C.E, Chin S.K. and Frincke D., 1998: "Ingetrating Security into the Curriculum" *Computer*, Volume 31, No 12
- [2] King Report, 2001: *The Code of Corporate Practices and Conduct*, (King Report), Institute of Directors, South Africa, version of July 2001.
- [3] LEWIS A., 2002: "Time to elevate IT security to the boardroom" *E-Secure*, Volume 1, Issue 1.
- [4] National Institute of Standards and Technology 2000: "*An Introduction to Computer Security.*" Online available: [www.nist.gov](http://www.nist.gov)
- [5] NIST- National Institute of Standards and Technology, 1989: "*Computer Security Training Guidelines.*" Also available online: [www.nist.gov/](http://www.nist.gov/)
- [6] Palmer M.E., 2001: "*Information Security Policy Framework: Best Practices for Security Policy in the E-Commerce age*" *Information Systems Security*, Vol.10 Issue 2.
- [7] Schou C.D., 2001: "*Information Security: International Curriculum Project*", Proceedings of the IFIP WG 11.8 Second World Conference on Information Secrutiy Education. Perth, Australia.
- [8] Siponen M.T., 2000: "*Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice*" *Information Management & Computer Security*, Volume 8, Issue 5.
- [9] Thomson M.E. and Von Solms R, 1998: "*Information Security Awareness: Educating you users effectively*" *Information Management & Computer Security*, Volume 6, Issue 4, pp 167-173.
- [10] Thomson M., 1998: "*Make information security awareness and training more effective.*" Proceedings of the IFIP, TC 11.8, First World Conference on Information Security Education, Kista, Sweden, pp 261-270.
- [11] Von Solms S.H., 2000: "*Information Security - The third wave?*" *Computer and Security*, Volume 19 Issue 7.
- [12] Von Solms S.H. 2001: "*Information Security - A Multidimensional Discipline*" *Computer and Security*, Volume 20 Issue 6. pp 504-508.
- [13] Wright M.A, 1998: "*The need for Information Security Education.*" *Computer and Security*, Volume 1998, Issue 8.

# **Appendix E**

**Article submitted for publication in  
Computers & Security, May 2006**

**Information Security Management:  
An Information Security Retrieval and Awareness Model for Industry**

E. Kritzinger  
Lecturer, University of South Africa  
PO Box 12995, Die Hoewes, 0163, Centurion, South Africa  
Tel: +27 12 429 8547  
Fax: +27 12 429 6848  
[kritze@unisa.ac.za](mailto:kritze@unisa.ac.za)

E. Smith  
Professor, University of South Africa  
School of Computing, University of South Africa,  
PO Box 392, UNISA, 0003, South Africa  
[smithe@unisa.ac.za](mailto:smithe@unisa.ac.za)

Elmarie Kritzinger is a Lecturer in Information Systems at the University of South Africa. She is currently completing her PhD in Information Security at the University of South Africa and has delivered a number of Information Security papers at national and international conferences.

Elmé Smith is an Associate Professor in Computer Science at the University of South Africa. Her research interests include IT risk management, security in healthcare, information security management and information security awareness. She completed a PhD (Computer Science) at the Rand Afrikaans University in 2000 and has delivered papers at various information security conferences on a national as well as an international level. She has also published a number of papers in accredited subject-related journals.

**Abstract:** The purpose of this paper is to present a conceptual view of an Information Security Retrieval and Awareness (ISRA) model that can be used by industry to enhance information security awareness among employees. A common body of knowledge for information security that is suited to industry and that forms the basis of this model is accordingly proposed. This common body of knowledge will ensure that the technical information security issues do not overshadow the non-technical human-related information security issues. The proposed common body of knowledge also focuses on both professionals and low-level users of information. The ISRA model proposed in this paper consists of three parts, namely the ISRA dimensions (non-technical information security issues, IT authority levels and information security documents), information security retrieval and awareness, and measuring and monitoring. The model specifically focuses on the non-technical information security that forms part of the proposed common body of knowledge because these issues have, in comparison with the technical information security issues, always been neglected.

**Keywords:** Information security; information security awareness; information security management; information security risk; information security threats; information security vulnerabilities.

## **1. Introduction**

In today's competitive business environment, information is the lifeline of many organisations. It should therefore be protected, secured and managed accordingly (Broderick, 2001; Finne, 2000; Posthumus & Von Solms, 2004; Squara, 2000). If, for any reason, information is compromised, the organisation can lose time, manpower, money and/or business opportunities (Dhillon & Moores, 2001; Whiteman & Mattord, 2003). This protection of information is called "information security". The primary goal of information security is to protect information and ensure that the availability, confidentiality and integrity of information is not compromised in any way (Aljifri & Navarro, 2003; Finne, 2000; National Institute of Standards and Technology, 2000; Pfleeger, 1997; Von Solms,

1999). *Information security management* is about ensuring the security of information through proactive management of information security risks, threats and vulnerabilities. Information security management should be built into day-to-day business operations instead of being treated as an optional extra (Lewis, 2000).

One important aspect that forms part of information security management, is *information security awareness* (Deloitte, Touche & Tohmatsu, 2005; Lewis, 2000; Nosworthy, 2000; Schultz, 2004; Thomson & Von Solms, 1998; Wood, 1995). Information security awareness is about ensuring that all employees in an organisation are aware of their role and responsibility towards securing the information they work with (Irvine, Chin & Frincke, 1998; Schultz, 2004; Thomson & Von Solms, 1998; Wright, 1998). According to (Deloitte, Touche & Tohmatsu, 2005), about 45% of global organisations do not sensitise their employees in respect of possible information security threats, and this lack of information security awareness could well lead to compromised information within the organisation. It is the responsibility of management to ensure that information security awareness policies and procedures are in place.

The purpose of this paper is to present a conceptual view of an Information Security Retrieval and Awareness model that can be used by industry in order to enhance the information security awareness of employees. The first part will be devoted to the presentation of a common body of knowledge for information security specifically suited to industry, which will be used as a basis for the proposed model. The second part will be devoted to identifying different stakeholders in a typical organisation and grouping these stakeholders according to their job category. Finally, the paper will culminate in proposing the concept of an Information Security Retrieval and Awareness (ISRA) model for industry.

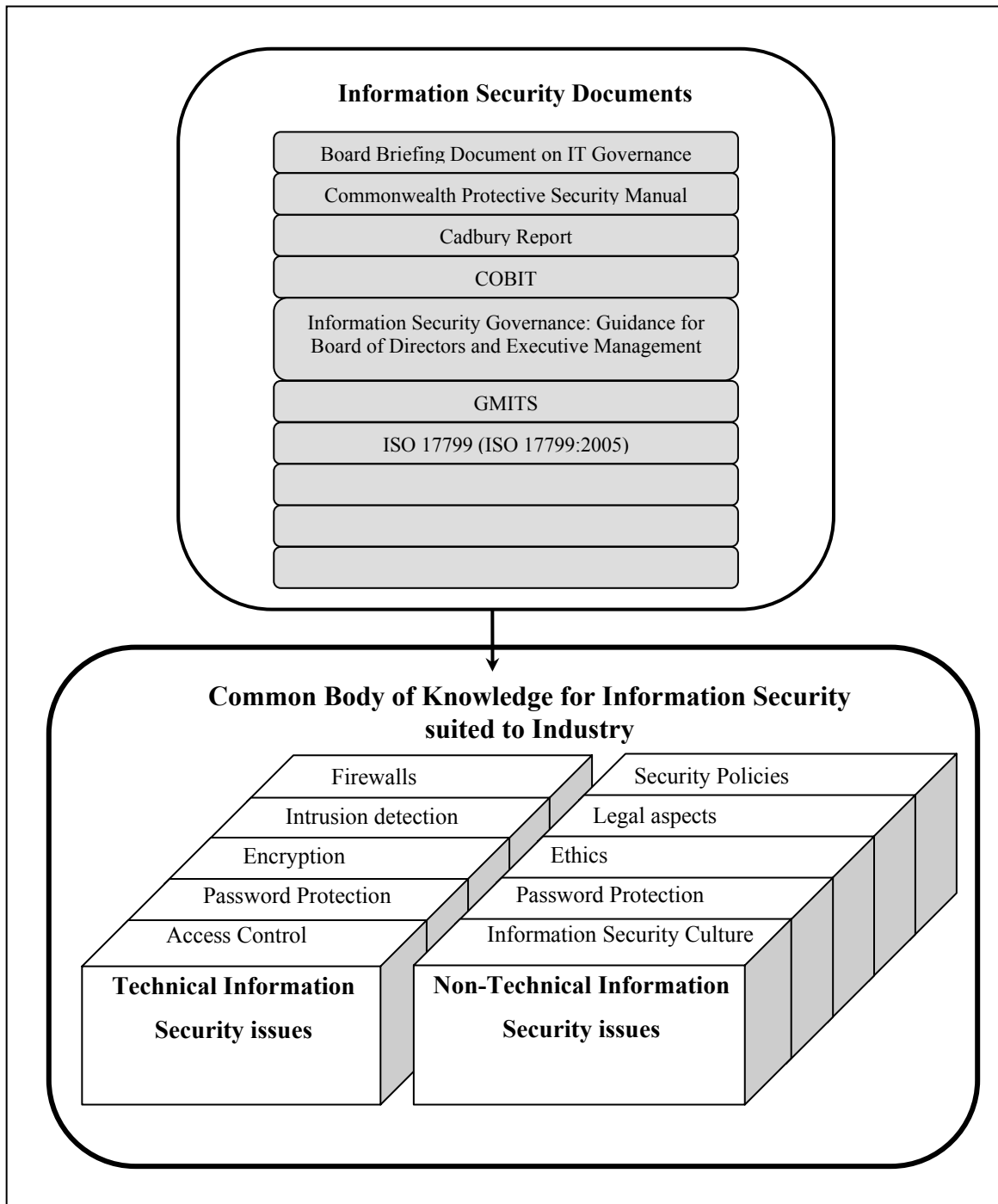
## **2. Common body of knowledge for information security suited to industry**

A common body of knowledge for information security is formed when information from around the globe is grouped together for the purpose of being used as a guideline on how to

secure information (Fraser, Kohane & Long, 1997). There are, however no universally accepted common body of knowledge for information security, though ongoing efforts are made to establish one (Crowley, 2003). A limitation that occurs in current developments of such a body of knowledge, is that it frequently focuses primarily on *professionals* in industry and leaves no room or opportunity for *low-level users* (such as end users) who require a scaled-down version of this knowledge (CSI/FBI, 2005; Wilson & Hash, 2005). The aim of the common body of knowledge that is developed as part of the basis for the Information Security Retrieval and Awareness model proposed in this paper is twofold: to focus specifically on users with little or no formal background on how to properly secure information they work with, yet also not to exclude professionals.

There is a further limitation in current developments regarding a common body of knowledge for information security suited to industry: – very often the non-technical, human-related issues such as ethics and legal issues do not receive as much attention as the technical issues (such as encryption) (Deloitte, Touche & Tohmatsu, 2005; Posthumus & Von Solms, 2004; Siponen, 2000a; Wright, 1998). The technical and non-technical issues of information security should be balanced to ensure that the *technical issues do not overshadow the non-technical issues* and that the human side of information security is adequately addressed when developing a common body of knowledge for information security suited to industry. Such a body of knowledge should be based on leading national and international information security documents to ensure that all information security issues (technical as well as non-technical) are addressed.

The common body of knowledge for information security tailored towards industry that is proposed in this paper therefore aims to address both these limitations in current developments of such common bodies of knowledge (see Figure 1).



*Figure 1: Common Body of Knowledge for Information Security suited to Industry*

Various state-of-the-art national and international accepted Information Security documents are used as basis for the proposed common body of knowledge for Information Security. These documents were compiled by top Information Security professionals and contain information regarding the implementation and management of Information Security issues. Due to paper length, the content of these documents are not discussed

further and the reader should consult the references for more detail (COBIT, 2001; GMITS, 2001; ISO/IEC177799, 2000; IT Governance Institute, 2001a; IT Governance Institute, 2001b; National Institute of Standards and Technology, 2000).

The proposed common body of knowledge is divided into technical information security issues and non-technical information security issues – as depicted in Figure 1. Firstly, this division will ensure that those information security issues relevant to *low-level users* can be identified more easily, because such issues will fall primarily into the non-technical side of the proposed common body of knowledge. Secondly, this division will ensure that *the technical information security issues do not overshadow the non-technical information security issues*. Note that the list of information security issues depicted in Figure 1 is not exhaustive, but merely an example of some of the information security issues involved.

The technical information security issues focus mainly on the technical-oriented knowledge and tools (such as encryption techniques) that are required to secure and protect information (Smith *et al.*, 2004). These issues are mostly confined to the technical departments and employees with proper information security knowledge and work experience. Their knowledge is usually obtained through formal qualifications, such as tertiary degrees/diplomas or industry-related information security courses.

The non-technical information security issues include all the non-technical-oriented knowledge that is required to secure and protect information and information systems. It includes issues such as ethics, legal issues and information security culture. This non-technical part can also be considered the management side of securing and protecting information and information systems. Its focal area involves the different effects that humans can have on the security and protection of information and information systems. These human influences can be classified as intentional or accidental, and they may originate from either outside or within an organisation.

Some information security issues may be part of both the technical and non-technical components of the common body of knowledge for information security suited to industry, for example password protection (see Figure 1). Password protection can be viewed as a *technical* issue in instances where technical personnel install software on the network to



regulate the use of passwords. On the other hand, password protection can be considered as a non-technical issue in a situation where it is up to the user to choose a secure password. In the majority of cases however, information security issues will be part of *either* the technical *or* the non-technical components of the common body of knowledge for information security suited to industry.

The Information Security Retrieval and Awareness model proposed in this paper will focus exclusively on the *non-technical* information security issues. The primary reason for this is that much research has already been done regarding the implementation of technical information security issues in industry. Research into non-technical information security issues, however, emerged only recently and the human-related information security issues have – in comparison with the technical information security issues – been neglected so far (CSI/FBI, 2005; Deloitte, Touche & Tohmatsu, 2005).

The state-of-the-art *national and international information security documents* and the *non-technical information security issues* of the proposed common body of knowledge for information security suited to industry constitute the first two building blocks of the Information Security Retrieval and Awareness model proposed in this paper.

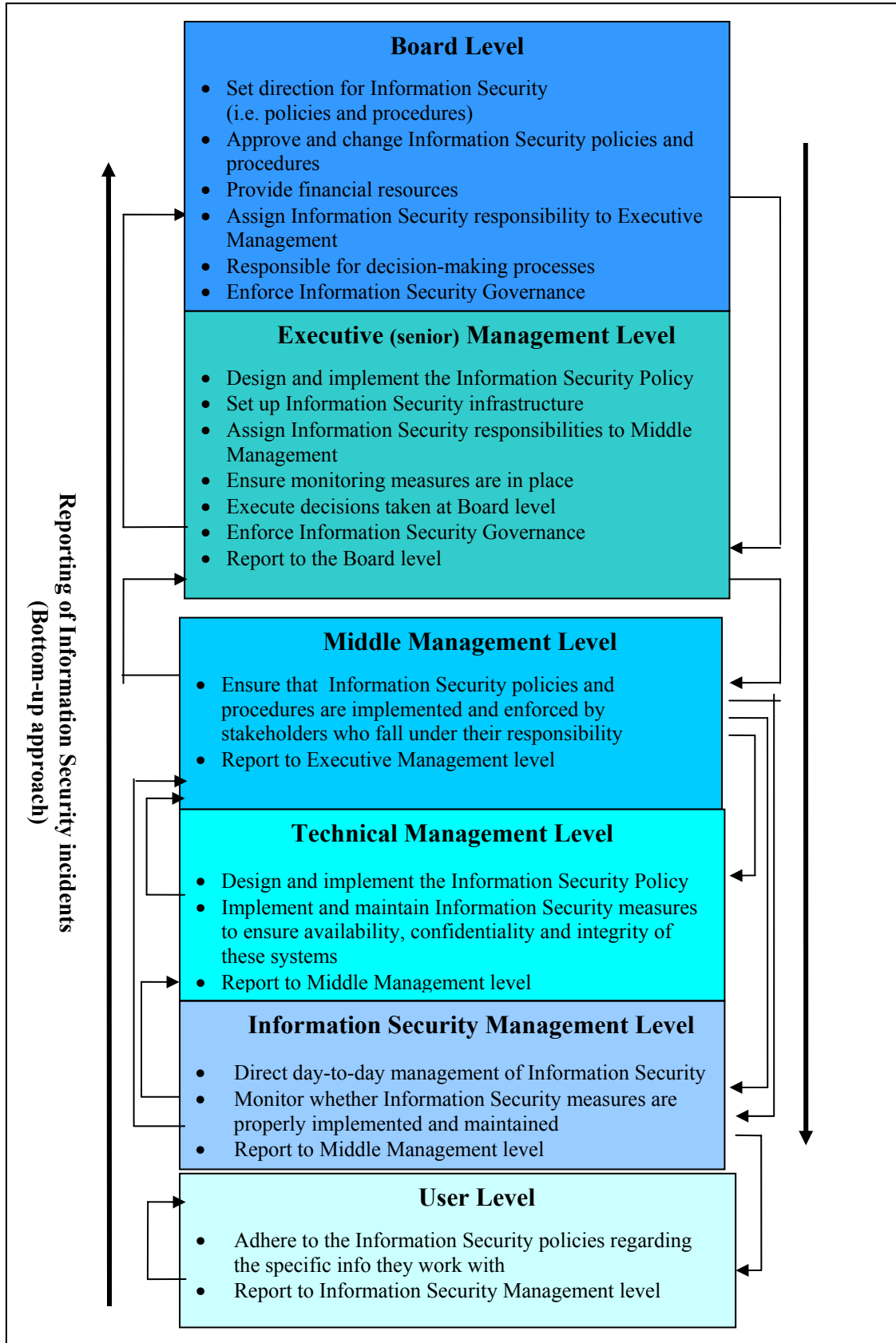
### **3. IT Authority Levels**

The third building block of the Information Security Retrieval and Awareness model is the IT authority levels. An IT authority level consists of a group of stakeholders who are the people who ensure the survival of the organisation (National Institute of Standards and Technology, 2000). The stakeholders are grouped together according to job category, for example executives (National Institute of Standards and Technology, 2000). Information security roles and responsibilities could be assigned to each group. This would ensure that a specific IT authority level is not overburdened with an enormous amount of information security documents that might include a large amount of irrelevant information. Instead, it would receive only the essential information needed to secure the specific information the IT authority level works with.

When creating IT authority levels according to job category, one should remember that job categories in organisations will differ from organisation to organisation and therefore the IT authority levels will also be different in different organisations (Kisin, 1996; National Institute of Standards and Technology, 2000; Siponen, 2001; Thomson, 1999; Whiteman & Mattord, 2003). For the purpose of this paper, the stakeholders in a typical organisation are grouped into six IT authority levels, as depicted in Figure 2. Figure 2 provides a summary of the primary responsibilities regarding information security for each of these IT authority levels.

The first IT authority level is the so-called Board level, which is widely recognised as the highest IT authority level of a typical organisation (Kisin, 1996; National Institute of Standards and Technology, 2000; Siponen, 2001; Thomson, 1999; Whiteman & Mattord, 2003). The Board is ultimately responsible for ensuring, through proper information security management, that information in the organisation is not compromised in any way. Only if the Board plays a proactive role in information security and information security management will the rest of the IT authority levels follow suit (National Institute of Standards and Technology, 2000; Whiteman & Mattord, 2003).

The second IT authority level is the Executive Management level and this will typically include the CEO, who is directly accountable to the Board. If the Executive Management level works very closely with the Board level, many of their responsibilities will overlap, such as ensuring proper Information Security Governance (i.e. a system or method by which companies are directed, controlled and managed) within the organisation (Andersen, 2001; IT Governance Institute, 2001a). The Executive Management level should therefore ensure that the decisions taken at the Board level are executed properly.



*Figure 2: IT Authority Levels*

Middle Management constitutes the third IT authority level and usually consists of different Heads of Departments or sections. This level should ensure that all information security policies and procedures are implemented correctly and that they are enforced by all stakeholders who fall under their responsibility (Nosworthy, 2000).

The fourth IT authority level is the Technical Management level that consists of stakeholders who are managers or technicians and who design and operate computer systems in the organisation (National Institute of Standards and Technology, 2000). The Technical Management level ensures that all technical aspects such as the latest information technologies and associated vulnerabilities and risks are addressed promptly and correctly by implementing and maintaining proper information security measures.

The fifth IT authority level is the Information Security Management level. This is widely recognised as the level that directs the organisation's day-to-day management of all the information in the organisation (International Federation of Accountants, 2000; Kisin, 1996; National Institute of Standards and Technology, 2000; Siponen, 2001). This level is primarily responsible for the assessment, management and monitoring of *security measures* in the organisation (Whiteman & Mattord, 2003).

The sixth and last IT authority level depicted in Figure 2 is the so-called User level. All stakeholders who fall under a specific user level have a responsibility for securing the information they work with (National Institute of Standards and Technology, 2000; Wood, 2004). These stakeholders should be made aware of all the information security rules and regulations that are available for securing such information (International Federation of Accountants, 2000; Kisin, 1996; Siponen, 2001; Thomson, 1999; Yngstrom & Bjorck, 2004).

A *top-down approach* should be followed when implementing information security. According to such an approach, the roles and responsibilities regarding information security are prearranged and enforced by an IT authority level that carries more authority than the level below. For example, it is the Board's responsibility to approve the Information Security Policy, whereas Executive and Middle Management are responsible

for implementing this policy in the organisation. Thus, all IT authority levels should be proactively involved in information security in the organisation.

The reporting of information security incidents, on the other hand, should follow a *bottom-up approach*. This implies that all IT authority levels should provide information regarding information security incidents directly to their appointed manager, in other words to an IT authority level that is one level up. For example, if a user detects a virus on his/her computer, he/she must immediately inform the Information Security Management level, who will handle the incident accordingly. The Information Security Management level, in turn, will report all security incidents to the next authority level, namely Middle Management. This approach will ensure that all information security situations and incidents are reported to the Board level, which has the authority to change the information security policies or procedures if necessary.

#### **4. Information Security Retrieval and Awareness (ISRA) model for industry**

The proposed Information Security Retrieval and Awareness (ISRA) model consists of three parts:

- The ISRA dimensions (non-technical information security issues, IT authority levels and state-of-the-art information security documentation)
- Information security retrieval and awareness
- Measuring and monitoring

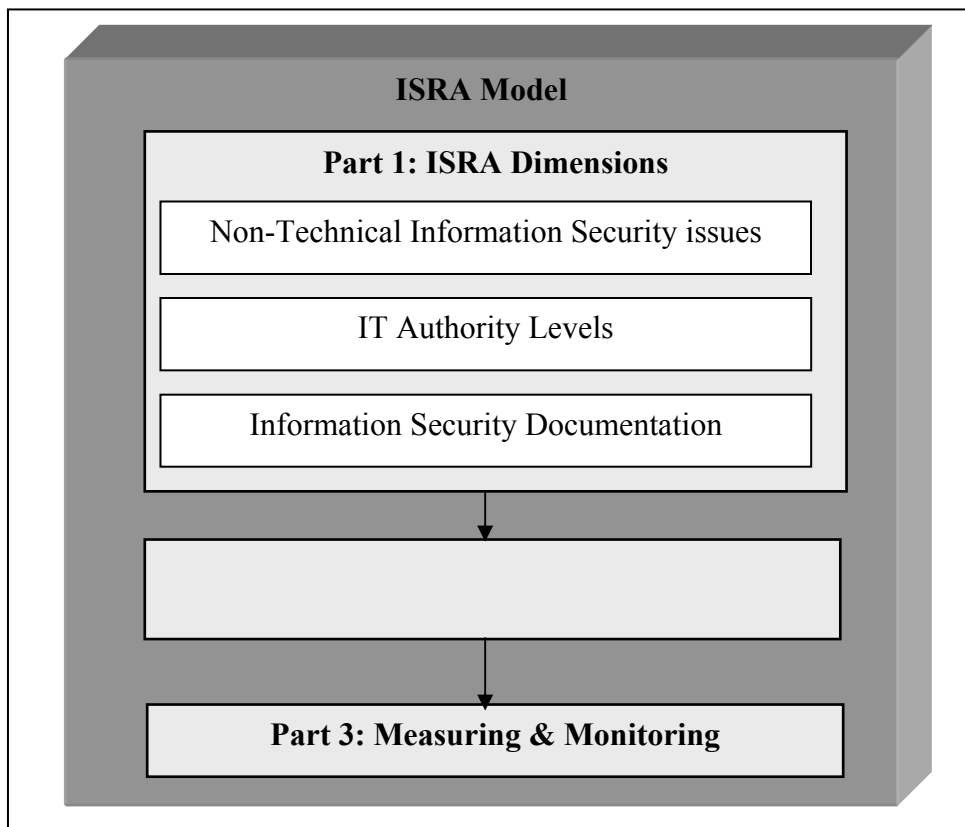


Figure 3: Conceptual view of the ISRA Model

#### 4.1 Part 1: ISRA Dimensions

The first part of the ISRA model (as shown in Figure 3) involves the ISRA dimensions, which form the basis of the model. This is the area in which all information regarding Information Security Awareness is accumulated. The ISRA model follows a three-dimensional approach by integrating the dimensions of *non-technical information security issues*, *IT authority levels* and *Information Security Documents*.

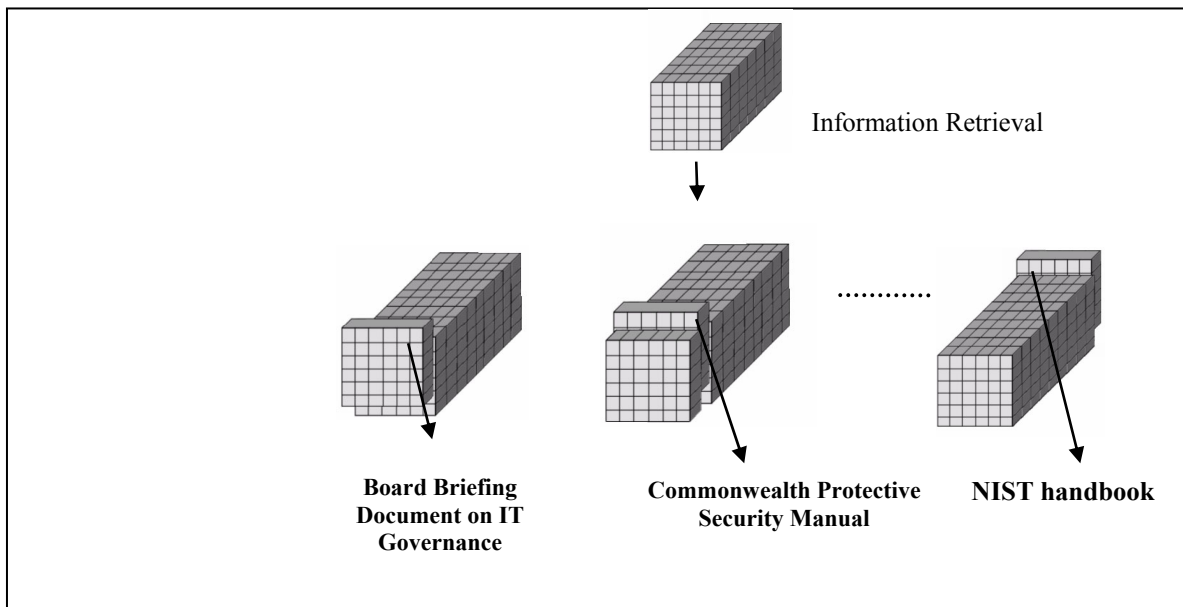
#### 4.2 Part 2: Information Security Retrieval and Awareness

The second part of the ISRA model, namely Information Security Retrieval and Awareness, will focus primarily on retrieving relevant information from the ISRA dimensions. This information will be requested by IT authority levels, depending on their information security awareness needs. The information retrieved in this part will be used to

enhance information security awareness among all IT authority levels, as well as to assist IT authority levels in decision-making processes. This retrieval of information is done by viewing the information within the ISRA dimensions from different angles. For example, specific information regarding an information security document can be obtained by viewing the ISRA dimensions from the y-axis, z-axis or a combination. Accordingly, three “slicing methods” will be used to retrieve relevant information from the ISRA dimensions.

#### 4.2.1 y-Slicing

The authors refer to the first slicing method as the y-slicing method. It extracts all requested information regarding individual information security documents from the ISRA dimensions. Each y-slice will represent one document, and will include the relevant information from both other dimensions (IT authority level and non-technical information security issues). Therefore, the y-slicing method will indicate which non-technical information security issues are important (relevant) and the IT authority level for which they are important, based on a specific information security document. This type of slicing method is depicted in the example illustrated in Figure 4.

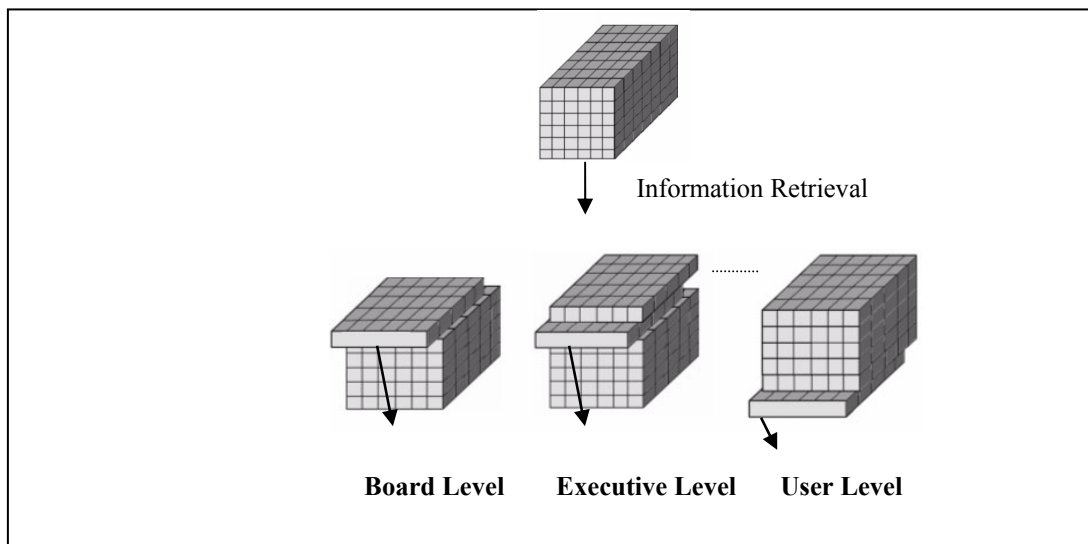


*Figure 4: y-Slicing*

In the example above, the first slice represents the information obtained from the Board Briefing Document on IT Governance, the second slice the information obtained from Commonwealth Protective Security Manual, and so forth.

#### 4.2.2 z-Slicing

The authors refer to the second slicing method as the z-slicing method, as this method will consider the information in the ISRA dimensions from the angle of the z-axis. Z-slicing extracts all the required information regarding the individual IT authority levels. In Figure 5 the ISRA dimensions are sliced to obtain relevant information about the specific non-technical information security issue that is highlighted, and the specific IT authority level that is involved.



*Figure 5: z-Slicing*

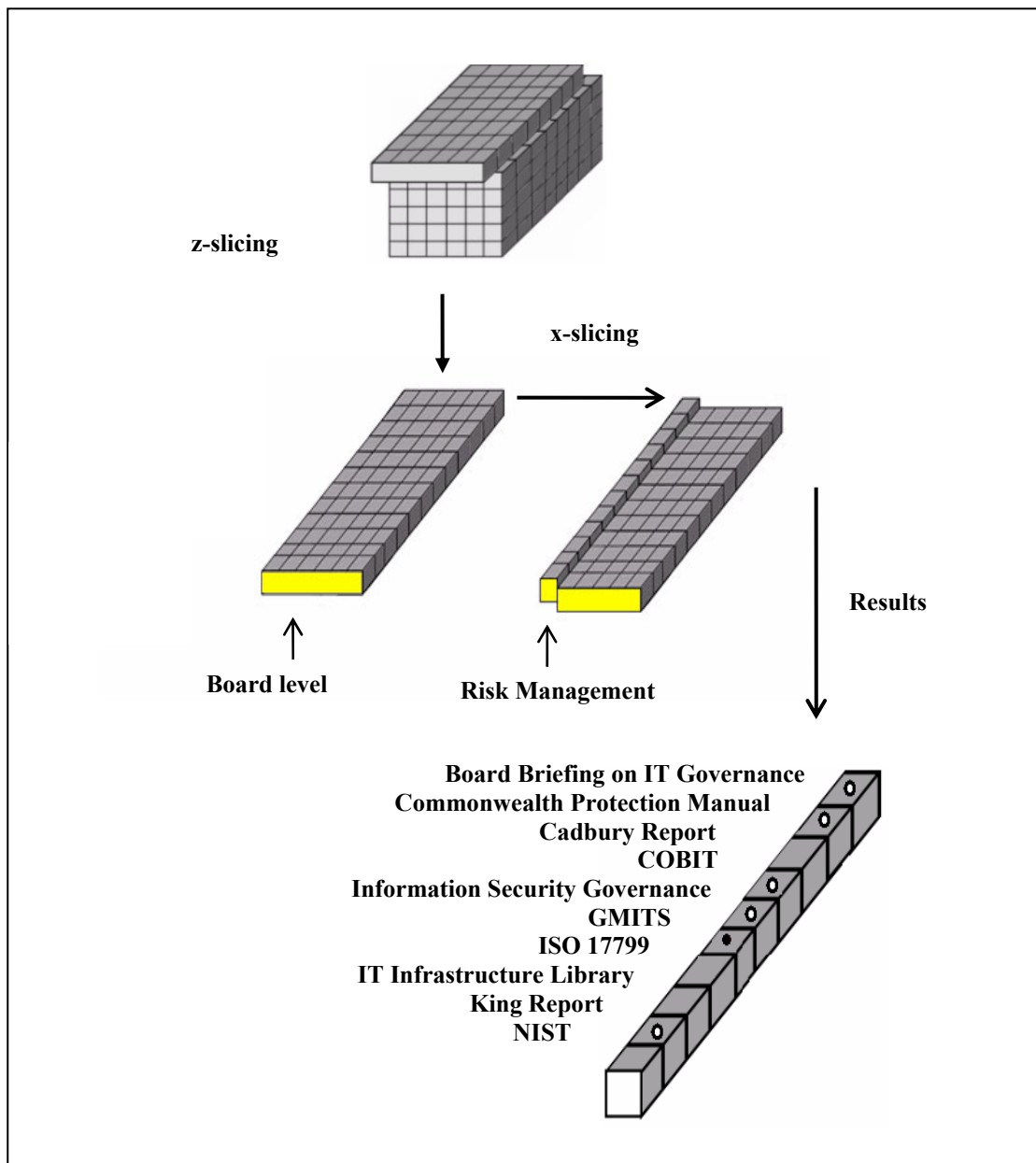
In the example illustrated in Figure 5, the first horizontal slice represents the Board level. This slice includes the different non-technical information security issues that have been identified by various information security documents and that are relevant to the Board level. A subsequent slice would represent the Executive level, and thereafter the other IT authority levels, down to the User level.



### 4.2.3 Combination-slicing method

The authors refer to the third slicing method as the ‘combination-slicing method’, as it combines x-slicing, y-slicing and z-slicing in a specific sequence, depending on the request of the stakeholder. The x-slicing method was not discussed separately, due to the fact that the information retrieved from this slicing method is not very significant on its own. However, x-slicing is used within the combination-slicing method to enhance both the y- and z-slicing methods. The combination-slicing method is therefore used when detailed information is required with regard to a specific IT authority level, non-technical information security issues and/or information security documents.

For example, consider a scenario where a stakeholder requests detailed information about the specific **information security documents that address risk management at Board level**. In this specific request, the sequence will be z-slicing, followed by x-slicing. (See Figure 6.) To obtain the requested information, a z-slice is firstly taken to identify the Board level as the relevant IT authority level. X-slicing is subsequently performed on the z-slice that was obtained to identify risk management as the relevant non-technical information security issue. In Figure 6, the ○ symbol is used to indicate the IT authority level that is *ultimately responsible* for that specific non-technical information security issue according to a given information security document. The ⊙ symbol is used to indicate the IT authority level that should ensure the *implementation* of a specific non-technical information security issue according to a given information security document. Finally, the ● symbol indicates that, according to a given information security document, a specific IT authority level should merely be *aware* of that non-technical information security issue. Thus – in the example in Figure 6, the results show that according to the Board Briefing Document on IT Governance, the Commonwealth Protection Manual, COBIT, Information Security Governance document and the King Report, the Board level is ultimately responsible for Risk Management, while – according to the GMITS document – the Board should simply be aware of Risk Management.



*Figure 6: Results of the zx-slicing method*

### 4.3 Part 3: Measuring and Monitoring

The third and last part of the ISRA model focuses primarily on measuring and monitoring the current information security awareness status in an organisation. The ISRA status in any organisation should be measured and monitored regularly to ensure that the latest information security awareness status is known at any given time (Von Solms & Von Solms, 2004a).

The purpose of the *measuring* process is to determine the level of information security awareness of each stakeholder in the organisation in respect of all the information security issues relevant to the IT authority level of that stakeholder. Such level of awareness is measured on a scale ranging from 0 to 100%, based on an Information Security Awareness Test that consists of a number of multiple choice questions related to a specific information security issue. These questions are based on the information contained in the information security documents that form part of the ISRA dimensions. The result of each test should be available immediately in order to indicate without delay whether there is a lack of knowledge regarding a specific information security issue. Each stakeholder must complete the relevant Information Security Awareness Test regularly so as to enhance his/her information security awareness and ensure that human-related information security breaches are minimised as far as possible.

The purpose of the *monitoring* process is to determine the information security awareness status within an organisation. The ISRA model also monitors this status by generating statistics based on the tests conducted during the measuring processes. These statistics are requested on an ad hoc basis by an IT authority level (such as the Board level) to determine if the organisation's information security awareness status is at an acceptable level and where problem areas lie. For example, the Board level may at any time request the display of percentages obtained for tests related to the latest information security policies. For each IT authority level, as well as for stakeholders within each IT authority level, the result of such a query will clearly display the number of stakeholders that are still not participating in the Information Security Awareness Test.

The monitoring process should also ensure that new information security issues or documents are incorporated into the ISRA model as soon as possible.

## **5. Conclusion**

This paper proposed a multi-dimensional Information Security Retrieval and Awareness (ISRA) model suited for industry. The proposed model consists of three parts: the ISRA

dimensions; Information Security Retrieval and Awareness; and Measuring and Monitoring. The first part (ISRA dimensions) follows a three-dimensional approach by incorporating non-technical information security issues, IT authority levels, and state-of-the-art information security documents. The second part (Information Security Retrieval and Awareness) focuses on retrieving relevant information from the ISRA dimensions. This information will be requested by the different IT authority levels, depending on their information security awareness needs. The information retrieved in this part will be used to enhance information security awareness among all IT authority levels, as well as to assist IT authority levels in making decisions about information security processes. The purpose of the third part of the ISRA model – Measuring and Monitoring – is to help organisations to measure the current status of information security awareness in the organisation, and to monitor the rapid developments in the information security field to ensure that all new information security issues are incorporated and addressed. A prototype of the ISRA model has in fact been developed and is currently being tested in industry.

## 6. References

- Aljifri, H. & Navarro, D. S. (2003). International legal aspects of cryptography. *Computers & Security*, 22(3): 196-203.
- Andersen, P. W. (2001). Information Security Governance. *Information Security Technical Report*, 6(3): 60-70.
- Broderick, J. S. (2001). Information Security Risk Management - When should it be Manged? *Information Security Technical Report*, 6(3): 12-18.
- COBIT (2001). *Governance, Control and Audit for Information and Related technology (COBIT)*, IT Governance Institute, ISACA, ISACF, 3rd edition, 2001, ISBN 1-893209-13-X.
- Crowley, E. (2003). Information Systems Security Curricula Development, in *Proceedings of the 4th conference on IT curriculum on IT Education*.
- CSI/FBI (2005). Computer Crime and Security Survey. Available at: GoCSI.com.
- Deloitte, Touche & Tohmatsu (2005). Global Security Survey. Available at: [www.deloitte.com](http://www.deloitte.com).
- Dhillon, G. & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security*, 20(8): 715-723.
- Finne, T. (2000). Information Systems Tisk Management: Key Concepts and Business Processes. *Computers & Security*, 19(3): 234-242.
- Fraser, H. S. F., Kohane, I. S. & Long, W. L. (1997). Using the technology of the world wide web to manage clinical information. Available at: <http://bmj.bmjournals.com/archive/7094ip1.htm>. 314 (No 7094).
- GMITS (2001). *GMITS: Guidelines for the Management of IT Security, Part 1: Concepts and models for managing and planning IT security*, ISO/IEC JTC1/SC27, PDTR 13335-1 (revision), version 28-11-2001.

- International Federation of Accountants (2000). Managing Security of Information.
- Irvine, C. E., Chin, S. C. & Frincke, D. (1998). Integrating Security into Curriculum. *Computer*: 25-30.
- ISO/IEC177799 (2000). Information security Management – Part 1: Code of Practice for information security management.
- IT Governance Institute (2001a). *Information Security Governance: Guidance for Boards of Directors and Executive Management*, ISBN 1-893209-27-X.
- IT Governance Institute (2001b). *Board Briefing on IT Governance*, ISBN 1-893209-27-X.
- Kisin, R. (1996). IT Security - Implementing "best practice". *Computer Audit Update*, 1969(1): 9-21.
- Lewis, A. (2000). Time to elevate IT security to the boardroom. *e Secure*, 1(1): 28.
- National Institute of Standards and Technology (2000). *An Introduction to Computer Security: The NIST Handbook.*, Special Publication 800-12.
- Nosworthy, J. D. (2000). Implementing Information Security In The 21<sup>st</sup> Century — Do You Have the Balancing Factors? *Computers & Security*, 19(4): 337.
- Pfhlieger, C. P. (1997). *Security in Computing*, Second edn, Prentice Hall, United States of America.
- Posthumus, S. & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23(8): 638-646.
- Schultz, E. (2004). Security training and awareness-fitting a square peg in around hole. *Computers & Security*, 23(1): 1-2.
- Siponen, M. T. (2000a). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1): 31-41.
- Siponen, M. T. (2001). Five Dimensions of Informstion Security Awareness. *Computers and Society*, 31(2): 24-29.
- Smith, E., Kritzinger, E., Oosthuizen, H. J. & Von Solms, S. H. (2004). Information Security Education, in *Proceedings of the WISE 4 Conference*, Moscow, Russia.
- Squara, D. (2000). LAN security will become a priority in the networks of tomorrow. Available at: <http://itweb.co.za>. 29 June.
- Thomson, M. (1999). Make information security awareness and training more effective, in *Proceedings of the IFIP, TC 11.8 Fisrt World Conference on Information Security Education*, Kista, Sweden.
- Thomson, M. E. & Von Solms, R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security*, 6(4): 167-173.
- Von Solms, R. & Von Solms, S. H. (2004a). From policies to culture. *Computers & Security*, 23(4): 275-279.
- Von Solms, S. H. (1999). Information Security Managment through Measurement, in *Prodeedings of the SEC99 conference*, Johannesburg, South-Africa.
- Von Solms, S. H. (2001a). Information Security - A Multidimensional Discipline. *Computers & Security*, 20(6): 504-508.
- Whiteman, W. & Mattord, H. J. (2003). *Principles of Information Security*, Thomson - Course Technology, Canada.
- Wilson, M. & Hash, J. (2005). Information Technology security awareness, training, education and certification. Available at: <http://www.itl.nist.gov/lab/bulletns/bltnoct03.htm>.
- Wood, C. C. (1995). Information Security Awareness Raising Methods. *Computer Fraud & Security*, June 1995: 13.

- Wood, C. C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security*, 2004(1): 16-17.
- Wright, M. A. (1998). The Need for Information Security Education. *Computer Fraud & Security*, 1999(8): 14-17.
- Yngstrom, L. & Bjorck, F. (2004). The Value and Assessment of Information Security Education and Training, in *Proceedings of WISE*.