A FRAMEWORK TOWARDS EFFECTIVE CONTROL IN INFORMATION SECURITY GOVERNANCE

M. VILJOEN

2008

A FRAMEWORK TOWARDS EFFECTIVE CONTROL IN INFORMATION SECURITY GOVERNANCE

By

Melanie Viljoen

Submitted in fulfillment of the requirements for the degree Magister Technologiae in Information Technology at the Nelson Mandela Metropolitan University

December 2008

Supervisor: Prof R Von Solms

DECLARATION BY STUDENT

FULL NAME: Melanie Viljoen

STUDENT NUMBER: 20310694

QUALIFICATION: M Tech IT

DECLARATION:

In accordance with Rule G4.6.3, I hereby declare that the above-mentioned dissertation is my own work and that it has not previously been submitted for assessment to another University or for another qualification.

SIGNATURE: _____

DATE: _____

ABSTRACT

The importance of information in business today has made the need to properly secure this asset evident. Information security has become a responsibility for all managers of an organization. To better support more efficient management of information security, timely information security management information should be made available to all managers. Smaller organizations face special challenges with regard to information security management and reporting due to limited resources (Ross, 2008). This dissertation discusses a Framework for Information Security Management Information (FISMI) that aims to improve the visibility and contribute to better management of information security throughout an organization by enabling the provision of summarized, comprehensive information security management information to all managers in an affordable manner.

ACKNOWLEDGEMENTS

I would like to thank Professor Rossouw von Solms for the time, guidance, insight and encouragement that he provided without which this dissertation would not have been possible. I would also like to thank the National Research Foundation for the funding that they provided. In addition, I would like to thank my family for their constant support and encouragement.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

Introduction

Chapter 1

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND

Information has and will continue to be seen as an extremely important asset in today's business environment (Bussiness Link, 2006; Pipkin, 2000, p. xix). Recognizing it as such, organizations must properly protect and secure it (Bussiness Link, 2006; ISO, 2006; Pipkin, 2000, p. 13). It is important to note that information security is not the exclusive responsibility of security experts with technical *savoir faire*. Every member of the organization plays a role and shares responsibility for the organization's information security (Pipkin, 2000). This is especially true of managers who are responsible for directing and controlling the assets for which they are answerable (Whitman & Mattord, 2004). If every member of an organization is to share responsibility for information security, it follows that every person, and especially managers in the organization, should have access to relevant management information about that organization's information security. It is, therefore, important that the appropriate information security management reports are available to people at all levels of an organization to support them to effectively direct and the control information security process.

1.2 DESCRIPTION OF PROBLEM AREA

Managers have the responsibility for directing and controlling the individuals under them in an organization (McLeod, 1983, p. 40). They will direct (let people know what they have to do) and control (make adjustments as they become necessary) in a way that will enable the organization to meet its objectives (Marchewka, 2003).

One of the important objectives of any organization should be information security (Whitman and Mattord, 2004). Information security is such an important concern that in many countries, a failure to demonstrate due diligence in this regard may lead to legal liability (Frazer, 2005; Whitman & Mattord, 2004). Brotby states that "senior

management will be increasingly seen as responsible and legally liable for failing the requirements of due care and diligence" (2007, p. 14).

Managers should, therefore, accept responsibility for directing and controlling information security concerns under their sphere of influence. As mentioned above, this is true for managers at all levels of the organization - strategic, tactical and operational (Von Solms & Von Solms, 2006; McLeod, 1983, p. 41). At the strategic level, managers are responsible for strategic issues, such as setting the vision and mission of the organization. The Board of Directors and Executive Management are typical at this level of management. Managers at the tactical level manage the implementation of directives received from the strategic level of management by formulating company policies, procedures and standards. The operational level is responsible for the implementation of the above. Managers who would contribute directly to an organization's information security programme would, therefore, include staff like the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), network and system administrators, who work directly with information technology (IT) or information security, members of the board and board committees that are responsible for the governance of the organization and managers of other departments of the organization (Corporate Governance Task Force, 2004). The Corporate Governance Task Force recommends that there should be a manager in each organizational unit responsible for information security concerns under the control of that organizational unit. They contend that management responsibilities include conducting risk assessments for their units, implementing policies and procedures and testing that information security controls and techniques are being implemented properly in their unit (Corporate Governance Task Force, 2004). If managers are going to have these responsibilities, it follows that they should be equipped with adequate information security management information. Pironti (2007) recommends a tiered reporting model to represent information to the different managers in the organization. As described below, he also suggests what information managers at each tier would typically want to see. He asserts that executive managers are likely to need "high-level, risk-oriented information that provides insight into costs and benefits associated with information security activities and infrastructure protection". Tactical managers will most often want to see the impact and effectiveness of controls

affecting them that have been put in place. Operational managers will probably be interested in ensuring that controls have been implemented properly and in the details and outputs of the measures.

The responsibility of all, and especially strategic managers, in the organization to properly manage and govern information security concerns should be clear. The *IT Governance Global Status Report* (2006), however, highlights a global lack of security governance. The report indicates that only 9% of the surveyed organizations have implemented risk management adequately, for example.

With the plethora of information security data that is needed to provide understanding into information security matters for various managers, automated systems to collect and analyse the data become necessary. There are various information security monitoring and reporting tools available. Insecure.org lists many of these (2006). Many of these tools are designed to gather and report on a specific subset of information security information. To illustrate: a tool called Nessus can be used very effectively to scan for and report on network vulnerability (2006), SNORT detects, reports on and often prevents network intrusion (Insecure.org, 2006) and Norton Antivirus is used to prevent and report on possible virus infections. These tools often do not furnish non-IT managers with the information security management information relevant to them in a manner that allows them to be able to effectively manage information security. A comprehensive view of the wellbeing of an organization's information security is achieved by taking into consideration the information provided by these tools collectively. Dashboard-type applications that make comprehensive summarized information visible to managers assist in this regard (Robinson). Progress has been made in the design of these types of tools. Some of these information security dashboards are discussed in Chapter 4 of this report. Smaller organizations can, however, often simply not afford such systems (Ross, 2008, p. 9).

*Taking into account the information above, it should be clear that there is a need for a framework that will facilitate the visualization of collated information security management information to all levels of management to support information security governance in a manner that can benefit smaller organizations***.**

It is believed that the dissertation and resulting framework will contribute to the work being done with regard to dashboards used for information security and information security governance. The key principles of the framework and the first version of the prototype system have been presented at the Human Aspects of Information Security and Assurance (HAISA) Conference, an international conference in Plymouth, England in 2007.

1.3 PROBLEM STATEMENT

It has been recognized that all managers should share responsibility for securing an organization's information resources. To be able to do this effectively, these managers should be equipped with relevant information security management information. There is no single tool, to the knowledge of the researcher, which accomplishes this in a manner that most smaller organizations with limited resources could realistically benefit from.

1.4 RESEARCH OBJECTIVES

There is, therefore, a need for a framework that will facilitate the visualization of collated information security management information to all relevant levels of management to support effective information security governance for organizations with limited resources.

There are tools, technologies and techniques like web services, data warehousing and visualization applications available that make it possible to develop applications that make this type of comprehensive, summarized information visible to managers. A framework for the development of such tools will be described in the proposed research project. A description of the tools, technologies and techniques that are used in the framework will be provided. A motivation for why they are suitable and the benefits associated with them are will also be presented.

Taking the above into account, the primary objective of this project is the development of a framework that will facilitate the provision of effective management information in the

governance of information security. The framework will be developed in such a manner that it can be used by smaller organizations with limited resources.

Secondary research objectives include:

- To compile a set of desirable characteristics of a framework to facilitate the provision of effective management information in the governance of information security;
- To devise which techniques and technologies are well suited for use in the framework;
- To motivate that the framework can be used in smaller organizations with limited resources;
- To develop a prototype system based on the framework as proof of concept.

1.5 RESEARCH METHODOLOGY

As mentioned above, the primary objective of this research project is the development of a framework that will facilitate the provision of effective management information in the governance of information security. The focus on governance and management of information security clearly implies that people are involved, and this further implies that there is emphasis placed on the meaning of what is being researched rather than on the measurement thereof. Therefore, the research philosophy followed in this project is predominantly phenomenological. The associated research methodology implies certain research methods to be used in a social scientific domain. The research methods to be used are highlighted below.

A literature review will be conducted to compile a set of desirable characteristics for a framework for the support of information security governance and to discover which technologies can be used to achieve these characteristics. Based on the findings of the literature review, a framework will be developed. Arguments will be presented to highlight how the framework meets the criteria identified in the literature review. A proof of concept prototype system, based on the framework, will be developed.

1.6 LIMITATIONS

Although this work will present a framework for information security management information to support information security governance, the dissertation will not provide an implementation methodology for the framework. For example, the framework promotes the use of standards based information security questionnaires, where managers are required to set the minimum performance levels that the organization is willing to accept for various security initiatives. This work does not, however, recommend which managers should be assigned the task of completing the questionnaire or what these levels of performance could be. In addition, with the framework, information security data is stored in a data warehouse. The data warehouse design is, however, not discussed in detail.

1.7 LAYOUT

The dissertation consists of 9 chapters. These chapters are briefly described in the following section. Figure 1.1 illustrates the layout of the chapters.

Chapter 1 – Introduction

Chapter 1 introduces the dissertation by describing the research problem and the objectives of the work.

Chapter 2 – Governance

This chapter briefly describes corporate governance, IT governance and information security governance. It highlights how these have altered organizations' views of accountability for information security.

Chapter 3 – Information security: roles and responsibilities

In Chapter 3, the importance of clearly defined information security roles and responsibilities will be explicated. Some of the information security responsibilities managers at the strategic, tactical and operational levels of management have, are then provided.

Chapter 4 – Information security reporting tools

Various existing information security tools are discussed in this chapter.

Chapter 5 – FISMI desirable characteristics

This chapter provides a list of the characteristics that would be desirable in a framework (FISMI) that makes information security information visible to managers throughout an organization. The list is compiled by studying characteristics of Security Information Management systems (SIMs), management information systems (MISs), decision support systems (DSSs), executive dashboards, compliance dashboards and continuous auditing tools.

Chapter 6 – Tools and techniques suited for use in FISMI

Information technology tools, techniques and design principles that are commonly used today make it possible to create ISG reporting tools that have the desirable characteristics described in Chapter 5. Some of these are briefly discussed in this chapter.

Chapter 7 – FISMI: A Framework for Information Security Management Information

A framework that will make collated information security management information visible to all levels of management to support information security governance (ISG) is described in this chapter. The framework is called FISMI – a Framework for Information Security Management Information. Before FISMI is described, some of the factors that motivate the need for such a framework are discussed.

Chapter 8 – Information security management information prototype

This chapter briefly describes a prototype system that has been implemented based on FISMI. The prototype system is called ISMIPS – Information Security Management Information Prototype System.

Chapter 9 – Conclusion

Chapter 9 draws conclusions based on the research presented in the preceding chapters.

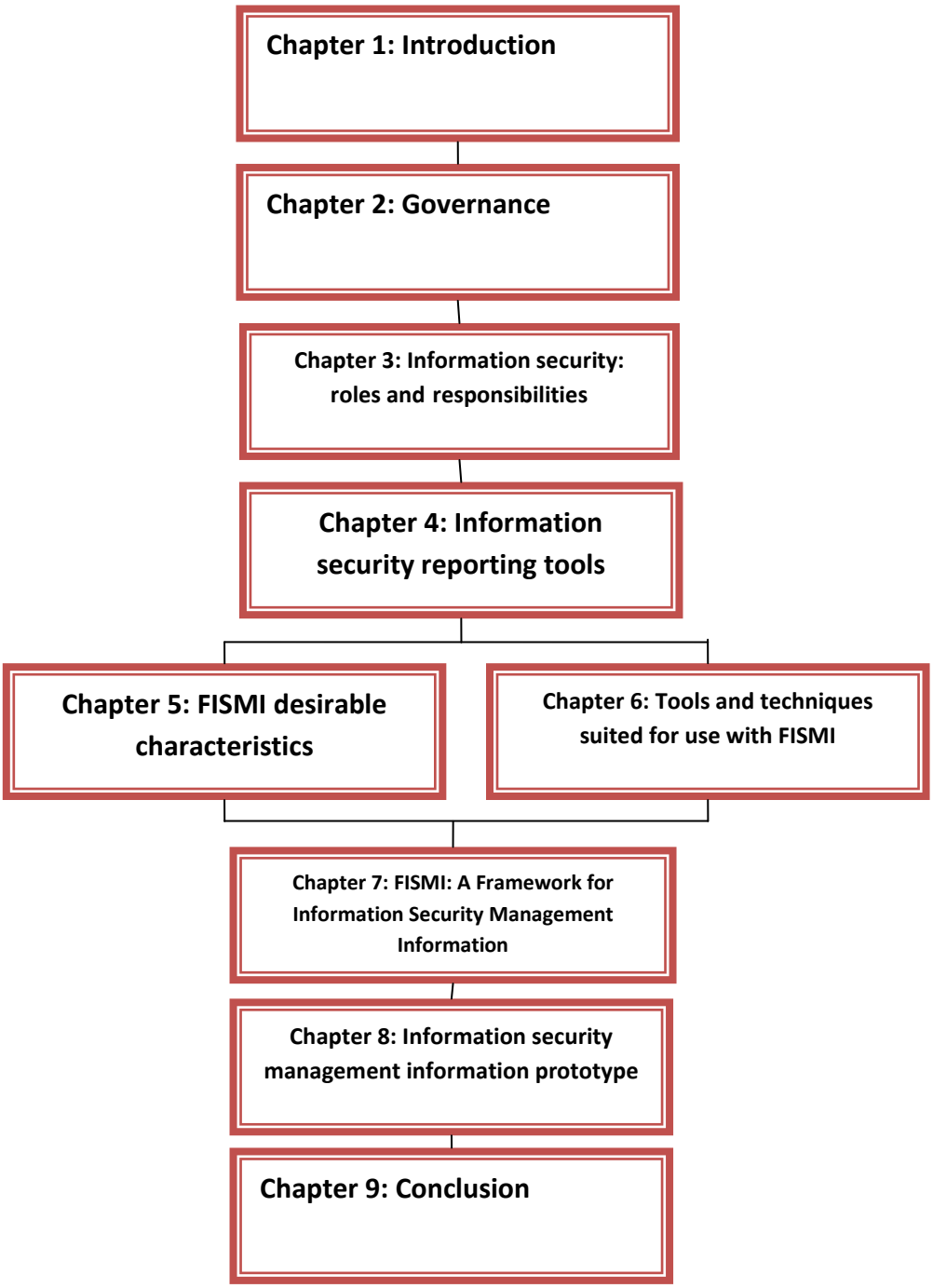


FIGURE 1.1 DISSERTATION LAYOUT

Chapter 2

Governance

CHAPTER 2: GOVERNANCE

2.1 INTRODUCTION

To be able to properly understand what will be required for a framework for the effective control of Information Security Governance (ISG), it is essential to understand what ISG actually entails. One of the main objectives of this work is to ensure that the framework that will eventually be described will aid all role players in ISG to meet their responsibilities. It is, therefore, important to have a good understanding of who in an organization should be involved in ISG. In the past, information security was often seen as the sole responsibility of Information Technology (IT) managers and staff. This view has changed and it is now widely accepted that everyone in an organization should contribute towards that organization's information security. Managers at the strategic level of management, such as CEOs and board members, are also being held increasingly accountable for their organizations' information security. Global developments in corporate governance and organizations' acceptance of it and its components, such as IT and ISG, have contributed to this change of attitude with regard to information security accountability.

This chapter briefly describes what corporate governance is. It also describes IT governance and ISG and how these have altered organizations' views of accountability for information security.

2.2 CORPORATE GOVERNANCE

Corporate governance is a subject that has had a marked affect on businesses worldwide (Wixley & Everingham, 2005, p. 2). Codes and guidelines for good corporate governance affect the structures, processes and mechanisms in place in big businesses. The following section will explain what corporate governance is and why it is so important. Once the need for good corporate governance is highlighted, the need for good IT governance and ISG as part of good corporate governance will also be discussed.

Corporate governance has to do with directing and controlling, or governing an organization to meet its goals and objectives (Institute of Directors, 2002). As this definition suggests, the purpose of corporate governance is to ensure that an organization meets the strategic objectives it has set for itself and meets the needs of the various organizational stakeholders, which often include government (Wixley & Everingham, 2005, p. 18). To accomplish this, corporate governance involves setting up relationships between a company's management, its board, and other shareholders and stakeholders (OECD, 2005, p. 11). It also involves providing the structures and mechanisms "through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined" (OECD, 2005, p. 11). There are similarities when it comes to describing good management and good governance in an organization. For example, definitions for both governance and management refer to the importance of directing and controlling. Peter Weill and Jeanne Ross (Weill, 2004, p. 8) highlight the difference between management and governance. They claim that governance is about *who* makes the decisions whereas management has to do with *making* and *implementing* those decisions. Ramani Naidoo (Naidoo, 2002, p. xiv) quotes Professor Robert Tricker as saying "If management is about running the business, governance is about seeing that it is run properly. All companies thus require management as well as governance".

There are several reasons organizations are so interested in corporate governance. In many instances, compliance to corporate governance guidelines, such as having a board, is a legal requirement (Congress of United States of America, 2002). Even in countries and instances where this is not the case, companies benefit from applying good corporate governance guidelines and principles. One of the main benefits is that companies that can demonstrate good governance are likely to attract more investors. Research has shown that investors are even willing to pay a premium for shares in a well-governed company as compared to a company with a similar financial record but is considered as being poorly governed (Weill, 2004). The converse is also true, and companies must realize that failing to demonstrate good corporate governance can have adverse consequences (Institute of Directors, 2002, p. 9). Countries should be concerned with creating a climate of good corporate governance since this can make a country "a magnet for global capital" (Institute of Directors, 2002, p. 12). On the other hand, the King Report shows that "if

there is a lack of good corporate governance in a market, capital will leave that market with the click of a mouse" (Institute of Directors, 2002, p. 9).

Considering the obvious importance of corporate governance, it should not be surprising that so much work has gone into developing principles and guidelines for it. Especially after some widely known corporate scandals in the 1990s (Wixley & Everingham, 2005, p. 14), the USA, the UK, Australia, South Africa and many other countries have developed or improved existing codes and guidelines for corporate governance (Mallin, 2006). Groups such as the Organization for Economic Co-operation and Development (OECD) and the Commonwealth Association for Corporate Governance (CACG) have also developed sets of principles of corporate governance that can be applied widely (OECD, 2005). Although there is no single code of corporate governance that can be applied to all organizations around the world at this stage, considering some of the general principles highlighted in a few of the abovementioned documents will give an enhanced understanding of what corporate governance involves.

The King Report on corporate governance in South Africa (Institute of Directors, 2002) identifies seven characteristics of good corporate governance. These are summarized below.

1. Discipline – Companies must show an awareness of and commitment to the principles of good governance, particularly at senior management level.

2. Transparency – Management should make the necessary information about a company's financial and non-financial aspects available in a candid accurate and timely manner.

3. Independence – Companies should have mechanisms in place to minimize or avoid possible conflicts of interest.

4. Accountability – Companies must have mechanisms in place to ensure that those who make decisions and take actions on specific issues are accountable for their decisions and actions.

5. Responsibility – Management should behave in a way that allows for corrective actions and for penalizing mismanagement so as to set the company on the right path.

6. Fairness – Companies must acknowledge and respect the rights of all groups that have an interest in the company and its future, including minority shareowners.

7. Social responsibility – Companies should respond to social issues and act in an ethical way.

Similar characteristics for good corporate governance are evident in other governance codes. For example, a study of the 15 principles outlined by CACG and the six principles outlined by OECD will show similar emphases on transparency, accountability and other of the characteristics for good governance listed above.

The OECD principles of corporate governance

- *A corporate governance framework should promote transparent and efficient markets, be consistent with the rule of law and clearly articulate the division of responsibilities among different supervisory, regulatory and enforcement authorities.*
- *A corporate governance framework should protect and facilitate the exercise of shareholders' rights.*
- *A corporate governance framework should ensure the equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders should have the opportunity to obtain effective redress for violation of their rights.*
- *A corporate governance framework should recognize the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises.*
- *A corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding a corporation, including the financial situation, performance, ownership, and governance of that company.*
- *A corporate governance framework should ensure the strategic guidance of a company, the effective monitoring of management by its board, and the board's accountability to its company and the shareholders.*

(OECD, 2005)

TABLE 2.1 THE OECD PRINCIPLES OF CORPORATE GOVERNANCE

A study of different corporate governance guidelines also makes it apparent that there are several structures and processes that are widely recognized as necessary for good corporate governance. These include a board of directors, board committees and audits, for example.

The board of directors and other executive managers of an organization have a key role to play when it comes to ensuring that the organization is governed effectively. Codes for good governance place a great deal of emphasis on the responsibilities and composition of boards. Organizations should, therefore, carefully make sure that their boards of directors are properly selected and that directors receive adequate induction into these companies. Directors should be made aware of their specific duties. Members of boards of directors must also realize that in their roles as directors, they will also carry potential personal liability (Wixley & Everingham, 2005, p. 26). The King Report makes this clear by showing that a board is "ultimately accountable and responsible for the performance and affairs of the company" and that it does not mitigate this responsibility when delegating authority to other managers or committees (Institute of Directors, 2002, p. 21).

A board of directors is often assisted by board committees. These are responsible for focusing on more specific governance issues and reporting back to the main board. In most organizations that follow principles of good corporate governance, there are usually at least audit, remuneration and nomination committees (Wixley & Everingham, 2005, p. 61).

Regular internal and external audits of an organization are also seen as a crucial part of corporate governance (Institute of Directors, 2002, p. 133).

The duties and responsibilities of the group described above will be described in more detail in the following chapter. The general roles of managers will, however, be briefly touched on as two important principles of corporate governance are addressed in the following paragraph.

Von Solms and Von Solms (2006) emphasize two core principles of corporate governance: direct and control. The direct-control cycle that they refer to involves all three levels of management: strategic, tactical and operational. At the strategic level, managers are responsible for strategic issues, such as setting the vision and mission of the organization. The board of directors and executive management are typical at this level. Managers at the tactical level manage the implementation of directives received from the

strategic level of management by formulating company policies, procedures and standards. The operational level is responsible for the implementation of the above.

Von Solms and Von Solms highlight that, according to corporate governance, one of the important functions of a board is to provide an organization with strategic direction. These directives are then expanded into policies, standards and procedures that are filtered down the different levels of management. They, in addition, draw attention to the fact that boards and executive managers also have a responsibility to control their organizations by ensuring that they operate in harmony with the directives provided by their boards and other internal managers and comply with externally imposed directives such as country and industry laws and regulations (Von Solms & Von Solms, 2006). The importance placed on the direct-control cycle by corporate governance principles will be of importance and referred to again in later chapters.

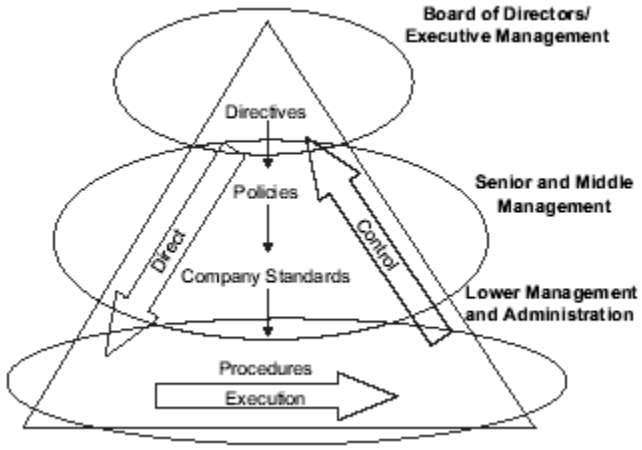


FIGURE 2.1 DIRECT-CONTROL CYCLE (Von Solms & Von Solms, 2006)

It should be clear from the above discussion that corporate governance is an important issue in business that should be of great interest to executive managers of companies worldwide. Corporate governance also has to do with more than merely the financial strategies and operations of a company. As stated earlier, one of the purposes of corporate governance is to ensure that companies meet their strategic objectives. The widely recognized importance of information as a strategic asset means that information technology governance (ITG) also plays a role in good corporate governance. In line with this, the following section will define what ITG is, how it is related to corporate

governance, why it is so important and some of the standards and mechanisms used to ensure it.

2.3 INFORMATION TECHNOLOGY GOVERNANCE

Information is an important strategic asset for businesses. As such, organizations often invest a lot of money in and time and effort on information technology. Often, however, organizations are disappointed with the outcome of these investments since many IT projects either completely fail or do not seem to add value to the organization (Weill, 2004, p. 17). For these and other reasons, IT governance has become an important concern for organizations. In this section the relationship between IT governance and corporate governance will be discussed. The need for IT governance and what it involves will also be considered. To be able to this, IT governance firstly will be defined.

IT governance definitions
IT governance: Specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT (Weill and Ross, 2004, page 8).
IT governance is the responsibility of the Board of Directors and executive management. It is an integral part of corporate governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives (ITGI, 2000).
IT governance is defined as: the distribution of IT decision-making rights and responsibilities among enterprise stakeholders and the procedures and mechanisms for making and monitoring strategic decisions regarding IT (Peterson, 2004).

TABLE 2.2 IT GOVERNANCE DEFINITIONS

2.3.1 WHAT IS IT GOVERNANCE?

There are many definitions of IT governance, some of which have been highlighted in Table 2.2. These definitions emphasize some key principles of ITG:

- ITG is an integral part of corporate governance and, as such, is of importance to executive managers and the board, not merely IT managers. ITG is not merely a technical issue (Brown, 2006; Peterson, 2004, p. 9);
- An important component of ITG is specifying who will make IT decisions and who will be held accountable (Fogarty, 2004);
- Two main objectives of IT governance are to *align IT with an organization's strategy* and thereby to *add value to the organization* (Van Grembergen, De Haes, & Guldentops, 2004, p. 7);
- ITG involves a set of structures, processes, procedures and mechanisms for making and monitoring IT decisions.

Before considering each of the above mentioned points in more detail, some reasons why ITG is viewed as a vital concern in the business world are addressed (Ali, 2006, p. 70).

2.3.2 ITG – WHY THE FUSS?

The importance of ITG is clearly linked to the importance of information technology in organizations today. No matter how positively or negatively individuals in an organization may feel about IT, most agree that in our information age, IT is vital to the continued existence of organizations (Raghuphati, 2007, p. 95). IT has become a basic necessity for businesses like electricity or people. As such, practically every business unit in any organization depends to some extent on IT to operate appropriately (Weill, 2004, p. 15). As Peterson points out, business models and IT have become "virtually inseparable" and boards and business executives cannot "delegate, avoid, or ignore IT decisions" since they cannot run a business without "depending on IT and the IT functions at some point in time" (Peterson, 2004, p. 8). Raghuphati also highlights the

growing importance of ITG as it becomes "increasingly difficult to distinguish organizational strategic mission from the IT that enables the mission" (Raghuphati, 2007, p. 95). In the words of Ingevaldson, "An IT system does not belong to IT. An IT system belongs to the user department" (Ingevaldson, 2006). Since IT has become so pervasive in many enterprises, ITG is also important to ensure that IT decisions are distributed among those who are responsible for the outcomes (Weill, 2004, p. 15).

As IT continues to introduce new opportunities and threats to entire enterprises, it is also important that effective ITG is in place so that enterprises can quickly respond to these developments (Weill, 2004, p. 15; Ali, 2006, p. 71).

Recognizing the importance of IT, many companies invest a great deal of money and time in it (Weill, 2004, p. 14). Managers are understandably discontented when many IT projects fail, or apparently do not add value to the organization (Weill, 2004, p. 17). Managers must, however, recognize the role that they should play in making sure that proper ITG guidelines are followed so that IT strategy is aligned with business strategy and thereby add value to the organization. Proper ITG should ensure that money and time spent on IT is spent wisely and produces the intended results.

ITG is a critical determinant of a company's success (Brown, 2006). Weill and Ross show that one reason why enterprises should focus on ITG is because ITG pays off. In a study they conducted, they found that for-profit firms with an above-average ITG performance had superior profits unlike firms with inferior governance but the same strategy (Weill, 2004, p. 14). They also found that top-performing firms paid special attention to ITG and used governance patterns that applied to their particular needs (Weill, 2004, p. 18). Apparent good ITG can also contribute to stakeholder confidence and a good image with the public (Raghuphati, 2007, p. 98).

On the other hand, Ali shows, based on a study of Schwartz and Woodhead's work, that lack of effective ITG can lead to "business losses, bad reputation, 'runaway projects', and inefficient operational activities" (Ali, 2006, p. 71).

After considering the above points that highlight the importance of ITG, it should be clear why Peterson says "Executives recognize that "getting IT right" this time will not

be about technology but about (shared) IT governance" (Peterson, 2004, p. 8). The next section will highlight some important aspects of ITG by elaborating on the principles of ITG derived from its definitions mentioned earlier in this chapter.

2.3.3 ITG – How Does It Work?

ITG is an integral part of corporate governance. It has been made clear from the outset of this chapter that ITG is a component of corporate governance. As mentioned earlier, organizations today are very dependent on IT to be able to compete in the market and to meet the strategies set. It is, therefore, impossible for organizations to completely address corporate governance without addressing ITG (Van Grembergen, De Haes, & Guldentops, 2004, p. 4). IT can also "be seen as a driver for enterprise governance" (Van Grembergen, De Haes, & Guldentops, 2004, p. 5). IT allows organizations to make full use of their information resources and to communicate strategy and other management decisions throughout the organization. Since ITG is part of corporate governance, it should be evident that the mode of corporate governance of an organization will also influence the mode of that organization's ITG (Sambamurthy & Zmud, 1999, p. 264).

One important implication of the fact that ITG is a corporate governance issue is that it is the responsibility of the board and executive managers. As shown earlier, members of the board must realize that the board does not mitigate its responsibility when delegating authority to other managers or committees (Institute of Directors, 2002; Peterson, 2004). This is true of ITG as well. Although the CIO and other technical managers will play a big part in ITG, the ultimate responsibility still lies with the board. The importance of executive management playing an active role in ITG has often been highlighted. After a study of different organizations, Weill and Ross found that there were seven characteristics that all top governance performers displayed. The most important indicator of good governance was that managers in leadership positions could describe ITG. The second and third most important characteristics, likewise, have to do with management involvement. They are:

- Senior managers engaged more often and more effectively in ITG and used formal communication mechanisms such as management announcements and formal committees;

- Senior managers were more involved in ITG. "The more involvement, the better the governance performance" (Weill, 2004, pp. 124-125).

Brown also references several studies that highlight the critical importance of executive managers sharing in ITG (Brown, 2006, pp. 145-148,152-153).

It has been established that due to the fact that ITG is part of corporate governance, it should be addressed at board level and should involve executive managers. According to the definitions mentioned earlier, an important aspect of ITG is creating decision and accountability frameworks for IT. We will now consider who else, besides boards and executive managers, should share in ITG.

An important component of ITG is specifying who will make IT decisions and who will be held accountable. There has been considerable attention given as to who should make what decisions. Weill and Ross describe who make ITG decisions based on "IT governance archetypes" (Weill, 2004, pp. 58-63). These are summarized below:

1. Business monarchy – senior business executives make IT decisions;

2. IT monarchy – IT professionals make IT decisions;

3. Feudal – Business units, regions or functions make IT decisions;

4. Federal – Executives (may include IT executives) and business groups make IT decisions;

5. IT duopoly – IT executives and one other group (CEOs, business unit leaders or business process owners or groups of key system users) make IT decisions;

6. Anarchy – individuals or small groups make their own decisions (Weill, 2004, pp. 58-63).

It is generally accepted that who makes IT decisions will be determined by the specific goals, composition and personality of the enterprise (Leung, 2004). It is clear that certain managers should always be involved to some extent. The above list shows the need for ***board*s** to take responsibility for ITG. In addition, the critical role of ***senior executive managers*** such as the CEOs and Chief Financial Officers (CFOs) is also shown. It is understandable that the ***Chief Information Officer*** (**CIO*)*** will also play an integral part in ITG. Taking into account how critical IT is to companies, Van Grembergen, De Haes and Guldentops suggest that ***IT committees*** be established to oversee this vital area. They refer to the importance of an IT strategy committee at the board level and of IT steering committees at the executive level (2004, pp. 22-23). Fogarty (2004) also shows that ***business managers*** play an important role in ITG.

In the next chapter, the specific roles and responsibilities of each of these parties will be discussed.

The need for good ITG as part of corporate governance has been established and certain structures that ITG has made important in organizations have been identified. Another vital component of corporate governance - ISG - and what it involves will now be considered.

2.4 INFORMATION SECURITY GOVERNANCE

The description of ISG will follow the same pattern used to explain corporate governance and ITG respectively in this chapter. Consideration will be given to what ISG is, why it is so imperative to organizations and how it is implemented.

2.4.1 WHAT IS INFORMATION SECURITY GOVERNANCE?

Von Solms defines ISG as: "Information Security Governance is an integral part of corporate governance, and consists of the management and leadership commitment of

- the board and top management towards good information security;
- the proper organizational structures for enforcing good information security;

- full user awareness and commitment towards good information security; and
- the necessary policies, procedures, processes, technologies and compliance enforcement mechanisms,

all working together to ensure the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people, etc) are maintained at all times" (Von Solms B, 2006, p. 167).

This definition highlights some important aspects of ISG. It shows that like ITG, ISG is part of corporate governance and as such is the responsibility of the board and top management (Von Solms B. , 2005; Burgert, 2004; Corporate Governance Task Force, 2004). This makes it clear that information security should not be regarded as a mere technical issue (Dodds & Hague, 2004). The definition also implies that boards and executives must realize that although the Chief Information Security Officer (CISO) and other employees may have certain delegated responsibilities for information security, the ultimate responsibility to govern it properly lies with them (Burgert, 2004; Williams, 2007; Dodds & Hague, 2004). As Williams says, "It is with the CEO and the board that the buck stops and in today's IT enabled and independent world, ignorance and denial are no longer options" (Williams, 2007, p. 11).

2.4.2 WHY INFORMATION SECURITY GOVERNANCE?

There are several good reasons that ISG should be taken seriously throughout all organizations. Some are listed below.

- The necessity for good corporate governance has become more apparent in the last couple of years and ISG is an integral part of good corporate governance. As a result, the role of ISG has been more recognized as vital for the proper management and governance of organizations. This point has been highlighted several times in this chapter.
- Information is a strategic business asset; therefore, the protection of this asset should receive enterprise-wide attention. It is easy to develop a good appreciation for ISG when one has a clear appreciation of how vital information is to

organizations today. That having been said, few would question the established importance of information to organizations. Information is recognized as a strategic business asset and as such must be appropriately protected. Initially efforts to secure an organization's information assets were mainly technical in nature (Von Solms B, 2000). It has, however, become evident that it is impossible to effectively protect this important strategic asset without addressing this issue at the governance level, taking into account the human aspects of information security. "Information security is as much about behaviour as it is about technical safeguards" (ITGI, 2007, p. 14). In line with this, ISG has become an established component of corporate governance, as shown in the previous section.

- Failure to employ good ISG can have very negative effects on organizations (Moulton & Coles, 2003, p. 580). Security breaches can effect entire organizations not just their IT department. Some of the consequences of security breaches listed by CobIT, an internationally accepted standard of good practice for ITG, include: competitive disadvantage, loss of business, reputational damage, poor morale, operational disruption and privacy breaches (ITGI, 2007a, p. 13).
- Failure to demonstrate due diligence with regard to ISG can have legal implications. Von Solms and Von Solms (2006a) highlight the importance of managers showing due care with regard to ISG by using best practice. Failure to demonstrate due care in this way can mean that boards and top managers can be charged with negligence. As the ones responsible for the proper governance of information security, members of the board and other chief executives can be held personally accountable for such failures (Von Solms B, 2006).
- Following good ISG guidelines leads to possible benefits for the organization (ITGI, 2007a, p. 8). Paying better attention to information security will improve an organization's "overall reputation and strengthen its security posture" (Corporate Governance Task Force, 2004, p. 7). The Corporate Governance Task Force (2004, p. 8) also claims "information security holds the larger promise of increased productivity, heightened customer satisfaction, and ultimately, greater brand loyalty."

2.4.3 Information Security Governance – How is it Accomplished?

ISG follows all the same principles as those described earlier for good corporate governance and good ITG. As such, two important principles of corporate governance mentioned earlier – direct and control – are also important for ISG. Von Solms' Direct-Control Model was introduced earlier but will now be used to show how ISG is implemented throughout organizations. It is, however, firstly important to identify the role players involved in ISG.

Williams makes it clear that in line with corporate governance principles, one of the key factors to ensure that security continues to get the attention it deserves from everyone in the organization is that roles and responsibilities be clearly defined (Williams, 2007, pp. 12-13). Establishing "a security management structure to assign explicit individual roles, responsibilities, authority, and accountability" is also one of the core principles of ISG as identified by the Corporate Governance Task Force (Corporate Governance Task Force, 2004, p. 2). In previous sections, the people and groups involved with corporate governance and ITG were identified. Since ISG is a part of corporate and IT governance, it should be apparent that those involved with corporate and IT governance will also have a role to play with regard to ISG. Some of the key role players involved with ISG are listed below. In this chapter, the role players are merely identified. The responsibilities of these individuals and groups will be dealt with in the next chapter.

1. **The board, the CEO and other senior executive managers.** The undeniable importance of the roles that these managers play in both ITG and corporate governance has been emphasized. When it comes to making sure that ISG is properly governed, their roles are not diminished. This has been made clear already.
2. **Committees.** Audit committees have been mentioned as one of the committees that is usually in place in organizations to promote good corporate governance. According to Williams, the audit committee will have an increasingly important role to play with ISG (Williams, 2007, p. 13). In the discussion about ITG, IT steering committees and IT strategy committees were also mentioned. In

organizations that have these committees in place, these committees will also obviously give attention to information security as part of the overall IT concern.

3. **The CIO.** The Chief Information Officer will obviously be concerned about information security and will play a role to ensure it (Williams, 2007, p. 14).
4. **The CISO.** As the title suggests, the Chief Information Security Officer will play a central role in ensuring that good ISG is followed.
5. **Line business managers.** These managers are the ones that know which of the information they own and work with is confidential and sensitive and will, therefore, play an important role in the ISG process (Williams, 2007, p. 14). Information security problems are often caused by people and not IT. HR managers (as part of this group of managers) could, therefore, contribute greatly to good ISG (Williams, 2007).
6. **Technical managers and staff.** As the people in the organization with the technical expertise to actually implement controls for information security, technical managers obviously play a vital role in the ISG process.
7. **Everyone else.** It is important to note that everyone in an organization plays a role in ensuring good information security (Corporate Governance Task Force, 2004, p. 14). Williams states that, "Ultimately, it is the responsibility of each and every employee to help ensure information security" (Williams, 2007, p. 12). Von Solms also highlights this fact by saying that "Information Security Governance therefore involves everyone in a company – from the Chairman of the Board right through to the data entry clerk on the shop floor and the driver of the vehicle delivering the products to the customer" (Von Solms B, 2006, p. 167).

The specific responsibilities and duties of these groups will be discussed in the next chapter. To be able to better understand the ISG process, the general duties of these managers as they relate to the direct-control cycle will be examined below.

As mentioned earlier, according to corporate governance guidelines, the board and executives are both responsible for providing the strategic direction of the company (directing) and ensuring that the company is meeting the objectives set (controlling). As shown in Figure 2.1, this direct control cycle affects every level of management in the

organization – the strategic, tactical and operational levels. Directives are filtered down through all levels of management and compliance is measured and reported on by all levels of management. Von Solms and Von Solms (2006) explain that the same is true for ISG.

The first role players in ISG (the board, CEO and other senior executives) listed above are at the strategic level. They produce a set of directives for ISG. Von Solms and Von Solms emphasise that these directives will be influenced by both a company's profile (its vision, the role that IT plays in the company, etc) and external factors like laws, regulations and external risks. The directives from the strategic level are passed to the tactical level. Here, managers such as the CIO, CISO and business line managers (like HR managers) use the directives to produce security policies, company standards and procedures. These documents are used by managers at the operational level (e.g. administrators) to produce administrative guidelines and procedures which are executed by the other staff. The above process explains how managers direct for ISG. Von Solms and Von Solms also highlight how the ISG process is controlled by bottom-up compliance reporting.

At the operational level, information security information is collected. At the tactical level, this information is compiled and integrated to produce reports that highlight the status of information security to the strategic level in an aggregated format.

FIGURE 2.2 DIRECT-CONTROL CYCLE

Any discussion about governance is incomplete if consideration is not given to internationally accepted governance frameworks. The importance of these frameworks and some of the most popular corporate governance, ITG and ISG frameworks will briefly be introduced in the next section.

2.4.4 GOVERNANCE FRAMEWORKS

Governance frameworks provide a standard of good practice that serves as a measuring yard for how well organizations are applying accepted governance principles. Good governance is therefore often coupled to governance frameworks. Earlier in this chapter reference was made to some corporate governance frameworks including the OECD's principles of corporate governance, CAGGs guide on corporate governance and the King Report on corporate governance.

There are also internationally accepted frameworks available for guidance in ITG. IT Infrastructure Library (ITIL) and Control Objectives for Information and related Technology (CobiT) are examples of such frameworks. CobiT provides metrics and maturity models that organizations can use to measure the achievement of their IT goals (ITGI, 2007). One of the IT areas that CobiT addresses is the area of ISG. It contains several information security controls that organizations should take into account. A document entitled CobIT Security Baseline: An Information Security Survival Kit has also been made available (ITGI, 2007a). In this document, "44 steps toward better information" are presented and the CobIT control objectives are mapped to ISO 27002:2005. Specific security guidelines are also provided for home users, professional users, managers, executives, senior executives and boards of directors/trustees.

ISO/IEC 27002:2005 The Code of Practice for Information Security Management (hereafter referred to simply as ISO 27002:2005) is also an internationally accepted standard of good practice for information security. The standard consists of 11 security control areas. These security areas are further divided into 39 main security categories which together contain 134 controls. By being able to demonstrate adherence to the guidelines provided by ISO 27002:2005 or other accepted frameworks, organizations will

be able to show due diligence and will be following a holistic approach to information security (Freeman, 2007; Von Solms & Von Solms, 2006a).

2.5 CONCLUSION

To be able to understand what will be required for a framework for the effective control of ISG, a good understanding of what ISG is, how it is achieved and who will be involved with it is necessary. ISG has been described in this chapter as an integral part of corporate governance and IT governance. These two subjects have, therefore, been described so as to be able to better understand ISG in context. Throughout the chapter, role players for corporate governance, IT governance and especially ISG have been identified. It has been clearly demonstrated that everyone in an organization, from board level down, should be involved with information security. IT staff are not the ones who are solely or even primarily responsible for ensuring an organization's information security. In the next chapter, the responsibilities these various role players have will be highlighted. The framework that will eventually be described will aid these role players to meet their responsibilities.

INFORMATION SECURITY: ROLES AND RESPONSIBILITIES

Chapter 3

CHAPTER 3: INFORMATION SECURITY: ROLES AND RESPONSIBILITIES

3.1 INTRODUCTION

As stated in the introduction chapter, the primary objective of this work is the development of a framework that will facilitate the provision of effective management information in the governance of information security. To enable a clear understanding of what such a framework should accomplish and to understand the need for such a framework, there must be a clear understanding of the context in which this framework will be used. The previous chapter, therefore, gave a brief overview of what governance and particularly ISG involves. This chapter focuses on the information security responsibilities of various managers involved with ensuring effective ISG. Understanding the responsibilities of these managers enables one to understand more clearly: the need for a framework to facilitate the provision of management information for ISG, what information security information such a framework should provide and how such a framework could be used.

Below, the importance of clearly defined information security roles and responsibilities will be explicated. Some of the information security responsibilities managers at the strategic, tactical and operational levels of management have are then discussed.

3.2 THE NEED FOR CLEARLY DEFINED ROLES AND RESPONSIBILITIES

It is extremely important for any organization to have clearly defined and well communicated information security responsibilities for all employees. Two statements supporting this fact are given below.

1. It is an integral part of good governance.

It is impossible to allege good governance unless everyone in an organization clearly understands what is expected of them. One of the fundamental requirements for governance, as discussed in the previous chapter, is to have clear roles and responsibilities assigned to all in the company. Consider some of the key points made in the previous chapter in this regard. Two of the seven characteristics of good corporate governance, according to King, are accountability and responsibility (Institute of Directors, 2002). IT governance is defined as the process of "specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT" (Weill, 2004, p. 8). Establishing "a security management structure to assign explicit individual roles, responsibilities, authority, and accountability" is also one of the core principles of ISG as identified by the Corporate Governance Task Force (Corporate Governance Task Force, 2004, p. 2). Having clearly defined responsibilities is, therefore, a part of corporate governance, ITG and ISG.

The fact that good governance prominently involves a clear statement of responsibility is, moreover, a conclusion that we draw rather naturally. Would any director be able to make a movie if every role was not assigned to the appropriate actor and the actor was not given a script with the lines that he would say? Would a conductor be able to get a band of the best musicians in the world to play a piece of music if the musicians did not know what music or instrument they were supposed to be playing? Then how could we expect to run an effective information security programme in an organization if everyone involved does not know exactly what is expected of them and how to do it?

2. It is acknowledged by reputable individuals and groups as important.

This can be seen by studying the quotes listed below.

- "The responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be explicit" (Swanson & Guttman, 1996).
- The right IT services can be delivered when there is "an organization suitable in numbers and skills with roles and responsibilities defined and communicated, aligned with the business and that facilitates the strategy and provides for effective direction and adequate control and takes into consideration … clear roles and responsibilities, … job descriptions" (ITGI, 2000, p. 27).
- "Organizations should establish a security management structure to assign explicit individual roles, responsibilities, authority and accountability" (Corporate Governance Task Force, 2004, p. 2).
- "The first step in designing a governance framework is to determine who makes the decisions and who is held accountable for the decisions" (Sandrino-Arndt, 2008, p. 37).

3.3 ROLES AND RESPONSIBILITIES

As shown above, governance has largely to do with an organization's responsibility to have the proper mechanisms and processes in place to ensure that the right people are making the right decisions. The processes of ISG should, therefore, address the problem of who makes what information security decisions and who is eventually responsible therefore. Organizations will govern their information security differently because each organization is different. There is, therefore, no way to stipulate exactly what information security responsibilities every user in the organization should have. That will be determined by how the company is governed. There are, however, certain key role-players in ISG that were identified in the previous chapter that will generally have certain information security responsibilities regardless of the governance structure chosen by the organization. These role-players include managers from all the accepted levels of management (strategic, tactical and operational) since ISG involves managers at every

level in an organization (Von Solms & Von Solms, 2006, p. 410). Figure 3.1 depicts some of these role-players. The roles and responsibilities of these role-players will be discussed below. Figure 3.1 will be used throughout the rest of the chapter to indicate the level of management and the specific manager whose roles and responsibilities are to be discussed in each section. As this is done, it is important to bear in mind the aim of this. The general responsibilities of different managers are considered so that the need for and requirements of a framework to facilitate the provision of management information for ISG is clearly understood. The aim is not to completely list every information security responsibility of every individual in the organization, but rather to provide some guidelines thereto.

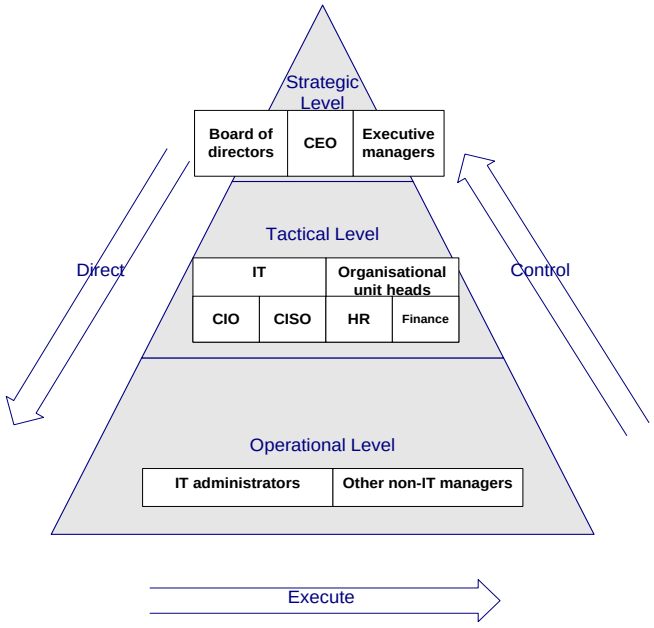


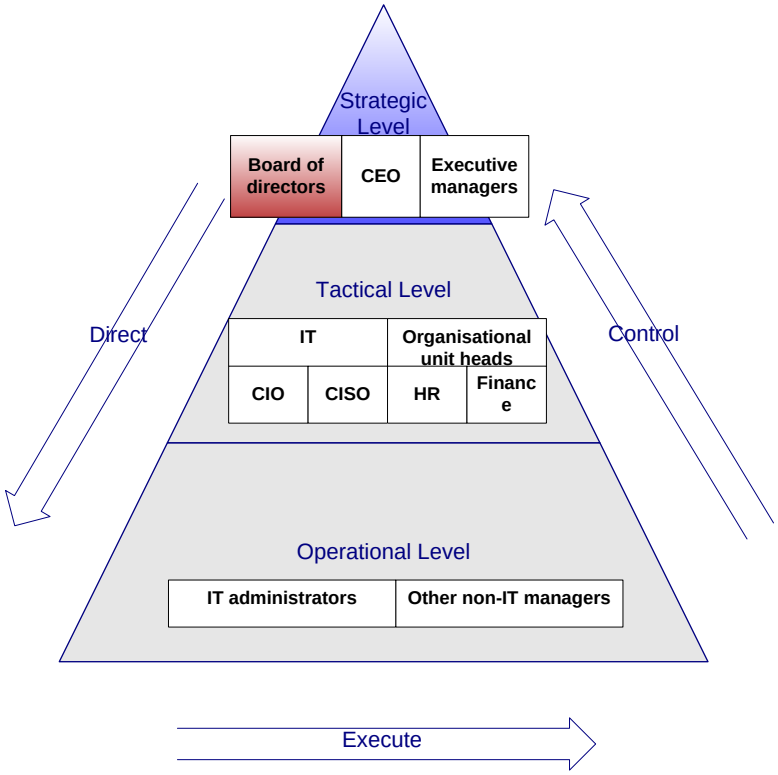
FIGURE 3.1 LEVELS OF MANAGEMENT

3.3.1 STRATEGIC LEVEL

Proper ISG is impossible without the involvement and support of strategic managers such as the board and CEO. The previous chapter highlighted this. It is fitting, therefore, that

work has been done to highlight the specific responsibilities that managers at this level should accept for proper information security (ITGI, 2007; Williams, 2007). CobiT Security Baseline v2 provides detail on the information security responsibilities that managers at this and other management levels are responsible for (ITGI, 2007). This document will be referred to extensively in this chapter.

3.3.1.1 THE BOARD



CobiT (ITGI, 2007, p. 36) provides an "Action List" for the board. The tasks on this action list are listed in Table 3.1 and motivated on the following page.

CobiT Security Baseline, 2nd Edition - Action List for Board members:

1. *Set Direction.*
2. *Assign responsibility to management.*
3. *Insist that management make security investments and security improvement measureable, and monitor and report on programme effectiveness.*
4. *Ensure that the board and/or audit committee clearly understand their roles in information security and how they will work with management and auditors.*
5. *Ensure that internal and external auditors agree with the board and/or audit committee and management on how information security should be covered in the audit.*
6. *Require a report of security progress and issues for the board and/or audit committee.*
7. *Develop crisis management practices, involving executive management and the board of directors, from agreed-upon thresholds onward.*

(ITGI, 2007, p. 36)

TABLE 3.1 COBIT SECURITY BASELINE, 2ND EDITION – ACTION LIST FOR BOARD MEMBERS

The Board must:

1. *Set direction.* As a group at the strategic level of management, it is understandable that one of the main responsibilities of the board of directors is to ensure that the organization has a well formulated strategy or plan of action (Wixley & Everingham, 2005, p. 14; Institute of Directors, 2002, p. 24). They are, then responsible for setting the strategic direction for the company. As is shown in the previous chapter, this responsibility includes setting direction for the organization's information security (Corporate Governance Task Force, 2004, p. 12; Von Solms & Von Solms, 2006). According to CobiT Security Baseline v2, the responsibility to set direction for information security includes the responsibility to "define cultural values related to risk awareness; drive policy and strategy; define global risk profile and set priorities" (ITGI, 2007, p. 36). The board is responsible for ensuring that a comprehensive information security

programme is developed and implemented (Corporate Governance Task Force, 2004, p. 13).

2. *Assign responsibility to management.* This is an extremely important action to be undertaken by the board. According to Williams, it is essential to establish clear responsibilities and decisions rights. This aids in ensuring that security is continually treated as a central concern (Williams, 2007, pp. 12-13). The following four actions on the action list (see table 3.1) further highlight the importance of this task. All four actions involve making certain that other groups are aware of and are meeting their information security responsibilities. It is, therefore, evident that although the board does not have to do everything necessary to ensure ISG, they do have to ensure that everything that has to be done is done by someone. Strategic managers cannot expect all other managers and members of an organization to act in a way that will contribute to the organization's overall information security if these employees are not aware of what they are expected to do in this regard. It is, therefore, imperative that there is a process in place to ensure that all relevant employees are assigned the appropriate information security responsibilities.

3. *Insist that management make security investments and security improvement measureable, and monitor and report on programme effectiveness.* The previous chapter highlighted the fact that two of the core principles of governance are to direct and control. The first of these emphasizes the need for the board to direct information security. The board, however, also has the responsibility to control the ISG process. Control involves measuring, monitoring and reporting on the level of compliance in the execution of directives provided (Von Solms & Von Solms, 2006, p. 410). As stipulated in step 6, the board is, therefore, responsible for requiring regular reports from management with regard to the information security programme's 'adequacy and effectiveness' (Corporate Governance Task Force, 2004, p. 13). Von Solms and Von Solms (2006, p. 411) draw attention to the fact that measurability is essential for effective control. This being the case, it

is vital that the board and other strategic managers make measurability a characteristic "at the centre of all directives, policies, standards and procedures produced" (Von Solms & Von Solms, 2006, p. 411). The board will, therefore, both require information security reports and ensure the reports are meaningful by ensuring that information security initiatives are measurable. The board is also responsible for evaluating how well information security investments are aligned with the organization strategy and risk profile (Corporate Governance Task Force, 2004, p. 12).

4. *Ensure that the board and/or audit committee clearly understands their roles in information security and how they will work with management and auditors.* As indicated by this step, audit committees are becoming increasingly responsible for non-financial aspects of business such as information security audits. A good relationship between the chair of the audit committee and information security professionals, such as the CISO, will be of great value in assisting the audit committee to understand their information security roles (Williams, 2007). The board is responsible for ensuring that this happens. It is understandable, however, that members of the board themselves also have the responsibility to ensure that they understand the board's responsibilities with regard to information security (ITGI, p. 8).

5. *Ensure that internal and external auditors agree with the board and/or audit committee and management on how information security should be covered in the audit.* As mentioned in the previous chapter, internal and external audits are important mechanisms associated with good governance practice. The aforementioned task is, therefore, important in contributing to successful ISG.

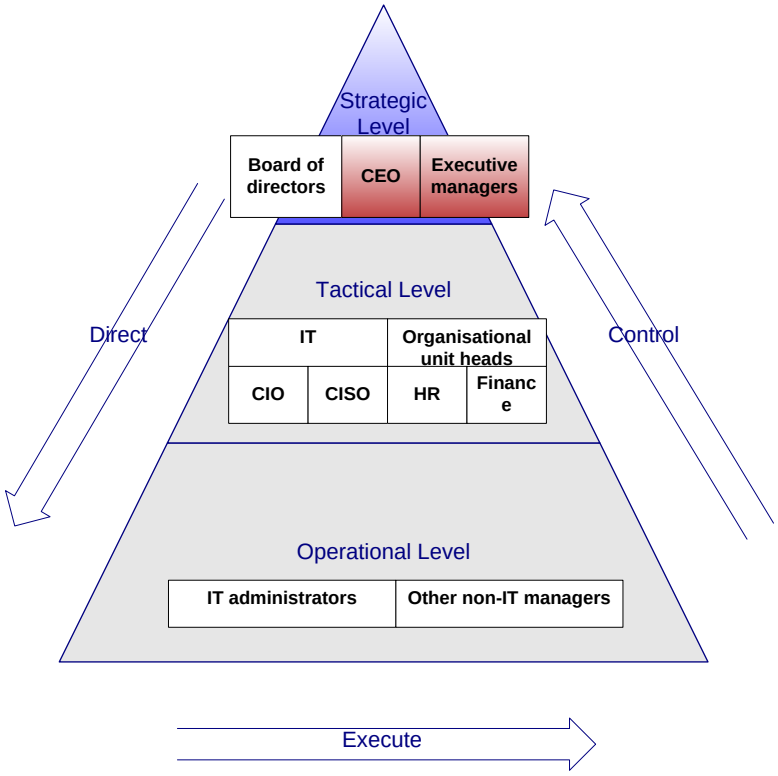
6. *Require a report of security progress and issues for the board and/or audit committee.* To be able to effectively direct and control information security, the board and other strategic managers need to be provided with timely security information. This is a fundamental principle for this research. A framework that

will facilitate the visualization of collated information security information to all levels of management would be helpful to the board and all other managers who have to be equipped with the appropriate information security information to support them in carrying out their information security responsibilities. The IT Governance Institute recommends that the board requires at least one annual information security report. This report should identify areas of risk and show the status of the security programmes related to this area (ITGI, p. 8).

7. *Develop crisis management practices, involving executive management and the board of directors, from agreed-upon thresholds onward.* The IT Governance Institute shows the importance of having both a formal business impact analysis (BIA) and a formal business continuity plan (BCP). Both these documents should be regularly reviewed and updated. There must, additionally, be evidence that the BCP is regularly tested and employees must know how to execute the BCP (ITGI, p. 12). The board will have to ensure that this happens. This step also points to the importance of having agreed-upon thresholds. Everyone in an organization, including the board and executive management, has to have an understanding of what is acceptable with regards to information security areas and what the company finds unacceptable.

From the above, it is clear that the board plays a key role with regard to ISG. The CEO and other senior executives, however, are responsible for carrying out a lot of the directives given by the board. Some of the information security responsibilities of these managers are discussed below.

3.3.1.2 THE CEO AND SENIOR EXECUTIVES



The CEO also plays a critical role in ensuring effective ISG. CobiT (ITGI, 2007, p. 34) provides an "Action List" for senior executives. The tasks on this action list are listed in Table 3.2.

Senior executives must:

1. *Establish a security organization and functions that assists management in the development of policies and assists the enterprise in carrying them out.* This item on the task list refers to some extremely important information security responsibilities. It highlights the fact that senior executives will be responsible for establishing a security organization and will play a role in the development of security policies.

Having a sound information security programme depends to a large extent on policy (Whitman & Mattord, 2004, pp. 106-107). Security policies should be developed in a manner that is consistent with the guidance given by accepted security standards such as ISO 27002:2005 (ITGI, p. 13). Policies should also be periodically reviewed and updated (ITGI, p. 9). It must, in addition, be clear that the organization's information security policy originates with and is approved by senior management (ITGI, p. 14).

The CEO must also make sure that the organization is structured and staffed in such a way that information security can be effectively managed and implemented. According to research by De Haes and Van Grembergen (2008, pp.26-27), there are seven "key minimum baseline" practices or functions that lead to good ITG. Included in these is making effective use of an IT steering committee and IT project steering committee and having the CIO report to either the CEO or COO. The CEO should, therefore, make sure that these mechanisms are in place and deal effectively with information security concerns. The CEO should, additionally, make sure that someone in the organization fulfills the role of a CISO (Corporate Governance Task Force, 2004, p. 13).

2. *Assign responsibility, accountability and authority for all security-related functions to appropriate individuals in the organization.* This step is in line with the responsibilities set out for CEOs in the Corporate Governance Task Force's call to action. It states that the CEO is responsible for "assigning the responsibility, accountability and authority for each of the various functions … to appropriate individuals within the organization" (Corporate Governance Task Force, 2004, p. 13). As shown earlier, it is essential that all employees are aware of their roles and responsibilities if information security measures are going to be effective. It is, therefore, important that these information security responsibilities are plainly 'defined and communicated' to all staff (ITGI, p. 26). The IT Governance Institute recommends that both the security awareness programme and job descriptions should be used to accomplish this. According to

them, there should be "clearly outlined statements of accountability in job descriptions" with regard to information security (ITGI, p. 16). The heads of each organizational unit also have to be made aware of their information security responsibilities. The executive team will have the responsibility of ensuring both "that each independent organizational unit develops and maintains an information security programme" and that the CISO "assists organizational managers concerning their information security responsibilities" (Corporate Governance Task Force, 2004, p. 14).

3. *Establish clear, pragmatic enterprise and technology continuity programmes, which are then continually tested and kept up to date.* The importance of having sound contingency plans which are well tested and communicated to employees was touched on in the previous section. The CEO would ideally be the champion of the contingency plan project. As such, the CEO would "support, promote and endorse the findings of" the contingency planning project (Whitman & Mattord, 2004, p. 86).

4. *Conduct information security audits based on clear process and accountabilities, with management tracking the closure of recommendations.* Information security audits are essential in ensuring effective information security. Jackie Bassett (2007, p.27) highlights some of the benefits of an information security audit, claiming that an effective audit "can enhance the organization's security stance, further its mission, and act as a catalyst that promotes sound IT governance." The need for internal audits was already implied in the previous section when discussing the board's responsibility to make sure that the audit committee understands its responsibilities with regard to information security. It is, furthermore, important that an organization has its network security regularly checked by a third party (ITGI, p. 15). The IT Governance Institute emphasizes the following important aspects with regard to the information security audit: security audits should be conducted by sufficiently trained audit staff at least once a year. These regular audits should cover both the security programme and the

way it is managed. It is, moreover, important that projects are established in response to audit recommendations and that these are controlled with proper project management techniques (ITGI, p. 25). The audit findings and recommendations must be reported in a way that is meaningful to the CEO and other senior executives. This could be done by linking the recommendation to the organization's strategic goals and objectives (Bassett, 2007, p. 27).

5. *Include security in job performance appraisals, and apply appropriate rewards and disciplinary measures.* It has already been established that senior executives, such as the CEO, have the duty to 'assign responsibility, accountability and authority for all security-related functions to appropriate individuals in the organization'. Senior executives, therefore, direct by making employees aware of what they should do about information security. As this item on the action list shows, senior managers must also apply control by monitoring how well employees are carrying out their responsibilities and take the proper reactive action.

6. *Develop and introduce clear and regular reporting on the organization's information security status to the board of directors based on the established policies, guidelines and applicable standards. Report on compliance with these policies, important weaknesses and remedial actions, and important security projects.* This item places the responsibility of providing information security reports to the board squarely on the shoulders of senior executives. The CEO or other senior executive should, therefore, ensure that there is a mechanism in place in the organization that ensures that the board receives clear and regular information security reports. To be able to do so, the CEO him or herself will also have to be aware of:
   - information security status based on policies, standards and guidelines,
   - the weaknesses and remedial actions (Corporate Governance Task Force, 2004, p. 13) and
   - the progress of important security projects.

In a similar manner, every other individual who is involved with a particular security project, or who has a role to play in ensuring effective information security, should get clear and regular information security information that pertains to them. An automated information security reporting tool could assist greatly in making this task easier.

7. *Ensure effective co-ordination amongst all of the organization's security and risk management functions.* This point once again highlights the central role the CEO plays in ensuring ISG. The CEO should ensure that the organization's enterprise risk management is properly handled. The CEO should ensure that information security risks are understood and mitigated (Williams, 2007, p. 12).

The abovementioned highlights that staff at the strategic level of management have a vital role to play in ISG. They should direct and control information security.

They direct information security in several ways. They ensure that the organization has a clear strategy for information security that is driven by executive management. They ensure that the organization has the ability to meet the strategic directives they have provided for information security by: making the appropriate resources available, making sure that the organization's culture and organizational structure promote good ISG, and by making sure that the necessary processes, functions and structures are in place to support information security efforts. They additionally direct for good information security by ensuring that everyone in the organization is sure of what they are required to do to contribute to the organization's information security.

Executive managers also control ISG. There are, once again, several ways in which they do this. For example, the above descriptions of these managers' responsibilities included requiring regular audits of information security and requiring that job appraisals encompass monitoring how well staff are meeting their information security responsibilities. Another imperative responsibility of these managers is that they should both require and contribute to meaningful information security reporting. It is important to highlight the active role that managers at the strategic level should play with regard to information security reporting. These managers do not passively wait for information

security reports. As per the items on the action list provided by CobiT Security Baseline v2, the board does not receive and read reports on information security progress. Rather they ***require*** these reports. Similarly, senior executives, such as the CEO, do not just receive information security reports. They rather '***develop*** and ***introduce*** clear and regular reporting on the organization's information security status to the board of directors based on the established policies, guidelines and applicable standards'. A framework that will facilitate the development of a reporting framework and associated tools that will provide effective management information in the governance of information security will, therefore, not only help strategic managers to monitor and control information security, it will also help them fulfill their responsibility with regards to information security reporting.

As has been shown repeatedly, one of the important ISG responsibilities of managers at the strategic level is to make sure that all other employees are aware of their information security responsibilities. Included in these other employees are managers at the tactical level such as the CISO, the CIO and executives of other non-IT units such as the financial and human resource departments. Some of the responsibilities of some of these tactical managers are discussed below.

CobiT Security Baseline, 2nd Edition - Action List for Senior Executives:

1. *Establish a security organization and functions that assists management in the development of policies and assists the enterprise in carrying them out. Assign responsibility to management.*
2. *Assign responsibility, accountability and authority for all security-related functions to appropriate individuals in the organization.*
3. *Establish clear, pragmatic enterprise and technology continuity programmes, which are then continually tested and kept up to date.*
4. *Conduct information security audits based on clear process and accountabilities, with management tracking the closure of recommendations.*
5. *Include security in job performance appraisals, and apply appropriate rewards and disciplinary measures.*
6. *Develop and introduce clear and regular reporting on the organization's information security status to the board of directors based on the established policies, guidelines and applicable standards. Report on compliance with these policies, important weaknesses and remedial actions, and important security projects.*
7. *Ensure effective co-ordination amongst all of the organization's security and risk management functions.*

(ITGI, 2007, p. 34)

TABLE 3.2 COBIT SECURITY BASELINE, 2ND EDITION – ACTION LIST FOR SENIOR EXECUTIVES

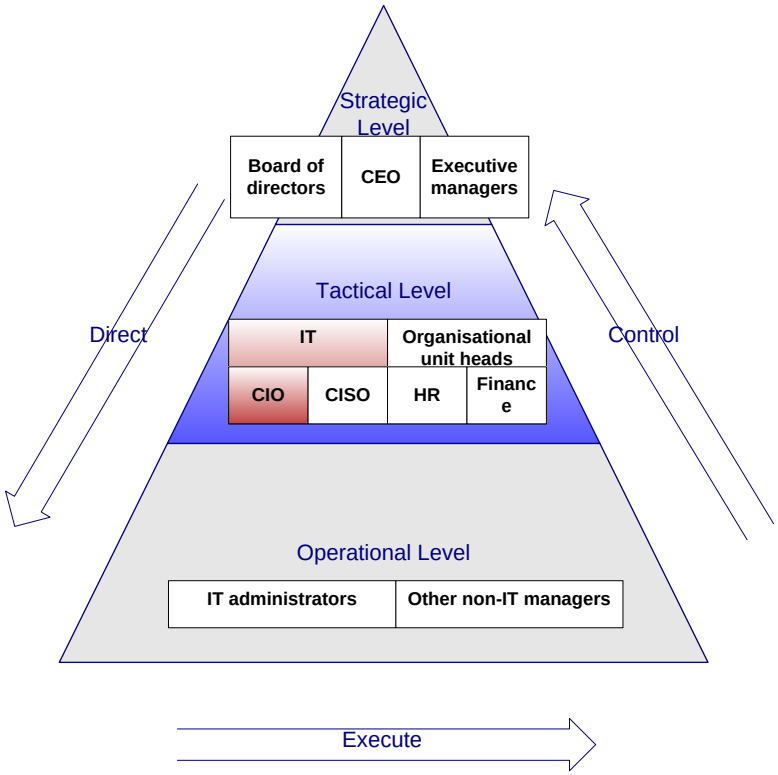
3.3.2 TACTICAL LEVEL

As explained in Von Solms' Direct-Control Cycle, actions of managers at this level are based on the input or directives originating from the strategic level. It is the responsibility of these managers to expand the directives received from strategic management into sets of appropriate information security policies, procedures and standards (Von Solms & Von Solms, 2006; Swanson & Guttman, 1996, p. 15). Although organizational structures vary from one organization to another, IT managers at the tactical level typically include

the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO). The intent of this work is not to give an exhaustive list of the information security responsibilities of these managers. It is, rather, to achieve a general understanding of their information security responsibilities so that the proposed framework to facilitate the provision of management information for ISG is developed based on an understanding of the needs of the users.

The responsibilities of typical IT managers at the tactical level are addressed firstly. Some information security responsibilities of a non-IT tactical manager, in this case the HR manager, are then discussed to illustrate some of the information security concerns of typical non-IT tactical managers.

3.3.2.1 THE CIO



As the title indicates the Chief Information Officer (CIO) will obviously play an important role in contributing to information security. According to Williams, "the CIO

will have a direct responsibility for information security insofar as it can be managed from within IT" (Williams, 2007, p. 14). Some of the high-level responsibilities of the CIO as compiled by Carika Olivier are listed in Table 3.3.

CIO – information security responsibilities:

1. *Formulate recommendations to the CEO on the strategic plans affecting the management of information in an organization.*
2. *Convert an organization's strategic plans into strategic information and information systems plans.*
3. *Collaborate with subordinate managers to develop plans of tactical and operational nature, enabling management of information and information systems. These would involve setting organizational information security policies and procedures.*
4. *Implement IT standards and policies.*
5. *Ensure that the IT budget is in line with the strategic aims and objectives of the organization.*
6. *Assess risks and ensure that risks are visible to the stakeholders.*
7. *Manage and verify IT processes and controls.*
8. *Respond to security breaches by investigating, mitigating and, if necessary, litigating these security breaches.*

(Olivier, 2006, p. 34)

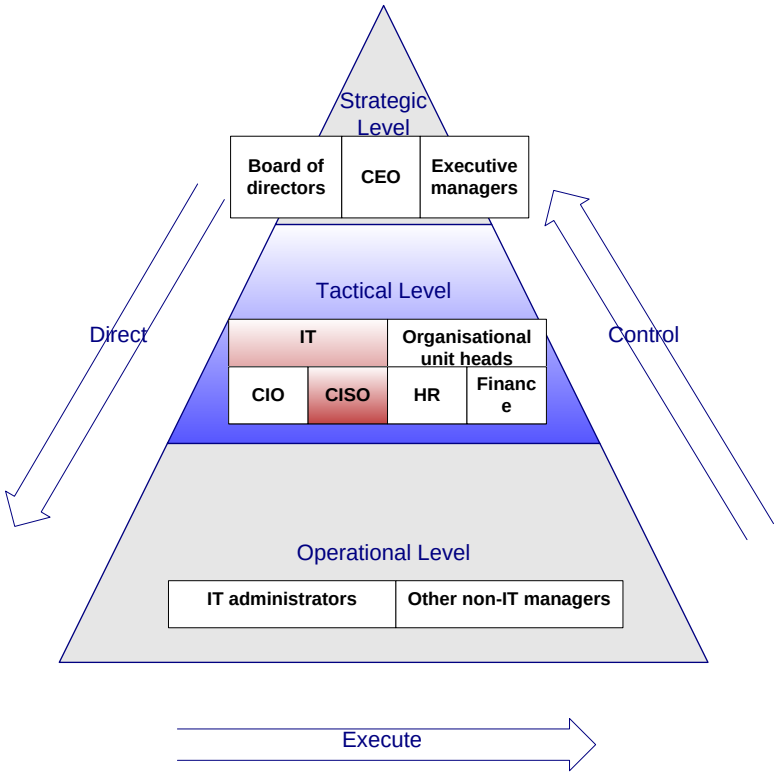
TABLE 3.3 RESPONSIBILITIES OF CIO (OLIVIER, 2006)

The CIO plays a vital role in ensuring information security, as can be seen from Table 3.3. The CIO contributes largely to the development of IT and information security policies, plans, standards, processes and controls. Not only is the CIO responsible for formulating the above mentioned documents, he or she is also responsible for ensuring that they are effectively implemented, managed and verified. This is a complicated job that requires a wide variety of technical, managerial and analytical skills. The CIO and other IT and information security professionals often make extensive use of information

security reporting tools to accomplish this task. These tools are discussed in the next chapter.

For the purpose of this work, it is important to highlight the specific responsibilities of the CIO. The CIO is responsible for making sure that managers at the strategic level, including the board and CEO, understand IT and information security to the degree that enables them to discharge their ISG responsibilities (Williams, 2007, p. 14). One of the ways that they can accomplish this is by making appropriate information about the state of various information security areas available to these managers. An automated tool that facilitates the provision of management information for ISG could prove of great value in this regard.

3.3.2.2 THE CISO



As the title, Chief Information Security Officer (CISO), implies, this employee plays an absolutely essential role in ensuring information security. As stated by Whitman and

Mattord (2004, p. 182), the CISO is "primarily responsible for the assessment, management, and implementation of the programme that secures the organization's resources." As can be seen by studying the above quote and a list of responsibilities for a CISO as compiled by Olivier in Table 3.4, the CISO is involved with directing, controlling and implementing an organization's information security. The CISO directs by contributing to the development and communication of the organization's strategic, tactical and operational plans. This employee then additionally controls information security by ensuring that all the necessary information security controls are functioning correctly. Like the CIO, the CISO will often make use of a variety of information security reporting tools to assist in controlling information security effectively. To be able to discharge these duties, the CISO will require strong technical security skills (Williams, 2007, p. 13). The CISO and other security professionals have the responsibility to constantly update their understanding of new threats and technologies that can affect the organization's information security (Karygiannis, 2008, p. 19).

Besides having strong technical and managerial skills to manage the responsibilities highlighted above, it is also becoming increasingly important that the CISO has good business understanding and skills (Williams, 2007, pp. 13-14). This can be seen from an additional information security responsibility of the CISO that Williams highlights. The CISO should work with business leaders and the board to gain commitment for information security (Williams, 2007, pp. 13-14; ITGI, p. 22). One of the ways that this can be done is by making sure that these strategic managers receive regular, meaningful information security reports. Another responsibility of the CISO is, therefore, to periodically report to strategic managers on the effectiveness of the security programme (Corporate Governance Task Force, 2004, p. 14).

CISO – information security responsibilities:

1. *The responsibility for overall information security management in an organization.*
2. *Collaborate with the CIO on strategic information security plans and collaborate with other security managers on operational plans.*
3. *Establish tactical plans.*
4. *Ensure protection for all physical aspects (for example, drafting policies and procedures for secure operations) and technical aspects (for example, risk assessments of IT assets) of an organization.*
5. *Ensure that information security breaches do not result from changes made to protect the organization.*
6. *Act as a representative of an organization in dealing with security strategy inquiries from customers and the general public.*
7. *Act as a representative of an organization in dealing with law enforcement agencies with regards to network attacks and employee theft.*
8. *Consider security requirements and business requirements of an organization to address any security risks to an organization while satisfying an organization's business goals.*

(Olivier, 2006, p. 35)

TABLE 3.4 RESPONSIBILITIES OF CISO (OLIVIER, 2006)

The CISO also has the responsibility to assist organizational unit heads to discharge their information security responsibilities (Corporate Governance Task Force, 2004, p. 14). As with the strategic managers, organizational unit heads can also be helped to carry out their information security responsibilities by receiving meaningful information security information that is appropriate to them. The CISO can, therefore, assist organizational unit heads by ensuring that they receive information security related information that assists them in discharging their information security responsibilities. A configurable automated tool that provides information security information to different managers may, therefore, be of great value to a CISO.

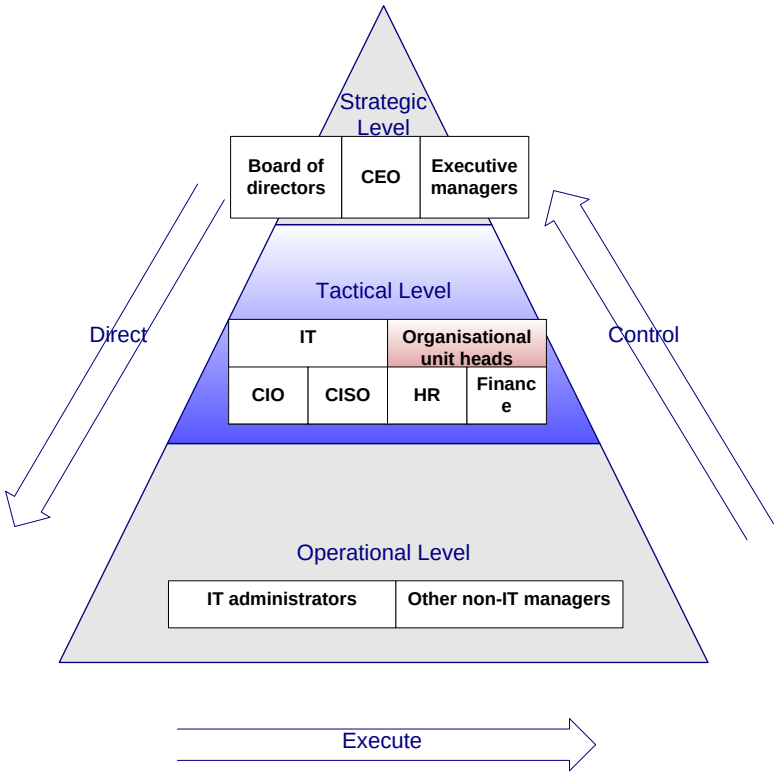
In summary of the above, it is important, in the context of this work, to highlight the following additional responsibilities of the CISO:

1. *Work with business leaders and the board to gain commitment for information security.*
2. *Assist organizational unit heads to discharge their information security responsibilities.*
3. *Provide strategic managers, like the board, CEO, and organizational unit heads, with the relevant meaningful information security information that will help these managers to discharge their information security responsibilities.*

It is important that the CISO clearly understands what his or her role and responsibilities include and that he or she receives at least annual performance evaluations (ITGI, p. 22).

The information security responsibilities of typical managers at the tactical level who operate primarily in the IT realm have been discussed. At this level of management, there are, however, many other organizational unit heads that may not have much IT knowledge, but who are major users of information and information technology resources. Their responsibilities for information security are considered next.

3.3.2.3 ORGANIZATIONAL UNIT HEADS



In describing the information security related responsibilities of other managers, it has been implied that heads of non-IT organizational units will have information security responsibilities. Why is this the case?

Charles Cresson Wood provides a reason why these managers should be integrally involved with information security. He describes how employees can be divided into three categories: information owners, custodians and users. He defines owners as those "ultimately responsible for certain information, including its security" (Wood, 1996, p. 34). He then shows that the information owners are typically the managers being considered here: tactical (middle level) managers, "for instance department or division heads" (Wood, 1996, p. 34). Organizational unit heads, as information owners, are, therefore, ultimately responsible for the security of information 'belonging' to them (Williams, 2007, p. 14; Wood, 1996; Corporate Governance Task Force, 2004, p. 14).

The Corporate Governance Task Force highlights six information security responsibilities of organizational unit heads. These are listed in Table 3.5.

Organization unit head – information security responsibilities:

1. *Assessing the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of the information and information systems that support the operations and assets under their control.*
2. *Implementing policies and procedures that are based on risk assessments and cost-effectively reduce information security risks to an acceptable level.*
3. *Determining the levels of information security appropriate to protect the information and information systems that support the operations and assets under their control.*
4. *Periodically testing and evaluating information security controls and techniques to see that they are effectively implemented.*
5. *Seeing that the organization has trained personnel sufficient to assist the organization in complying with the requirements of … policies, procedures, standards and guidelines.*
6. *Seeing that all employees, contractors and other users of information systems are aware of their responsibilities to comply with the information security policies, practices and relevant guidance appropriate to their role in the organization.*

(Corporate Governance Task Force, 2004, p. 14)

TABLE 3.5 CORPORATE GOVERNANCE TASK FORCE – RESPONSIBILITIES OF ORGANIZATIONAL UNIT HEADS

Wood and Williams elaborate on how and why heads of organizational units should be involved with risk assessments for their units and for determining the levels of information security appropriate for the information and information systems of their units. In many cases, these managers are the only ones who will be able to clearly classify which of the information they use is sensitive, confidential or critical (Williams, 2007, p. 14). It is, therefore appropriate that they are responsible for "making decisions about the sensitivity and criticality of information, identifying user access requirements,

determining an acceptable level of risk for both the information and the system that processes it and selecting appropriate controls for the information" (Wood, 1996, p. 34).

As implied earlier, organizational unit heads will rely on the support and assistance from security professionals in discharging their information security responsibilities (Corporate Governance Task Force, 2004, p. 14; Williams, 2007, p. 14). This support could include the provision of the appropriate information security information for that organizational unit.

Each independent organizational unit should also report to the proper senior executive about the effectiveness or deficiencies in the security programme. (Corporate Governance Task Force, 2004, p. 16) Another important responsibility of the organizational unit head will, therefore be, to ensure that, as far as it depends on them, the information security information from their department is properly reported.

It is, once again, important to highlight that the organizational unit head has the responsibility to both understand his or her own information security responsibilities and to ensure that other individuals in that organizational unit are aware of their information security responsibilities. As stated earlier, the IT Governance Institute recommends that information security responsibilities and accountabilities be clearly outlined in job descriptions (ITGI, p. 16). Despite the clear importance of this fact, it appears that many organizations do not explicitly include information security responsibilities in their non-IT employee's job descriptions.

A search for posts for a human resource manager was conducted on 14 May 2008 on the job search engine *Monster* (http://www.monster.com/). In the occupation drop-down list "General/Other human resource" was selected and the keyword "manager" was entered. The search resulted in 1829 hits. The search was then modified so that 'manager' and 'information security' was entered in the keyword field. Only one hit resulted. The post was for a human resource manager in a company that 'makes personal digital interactions secure and easy'. In the job description, the company lists various responsibility categories such as compensation and salary administration, staffing, employee relations,

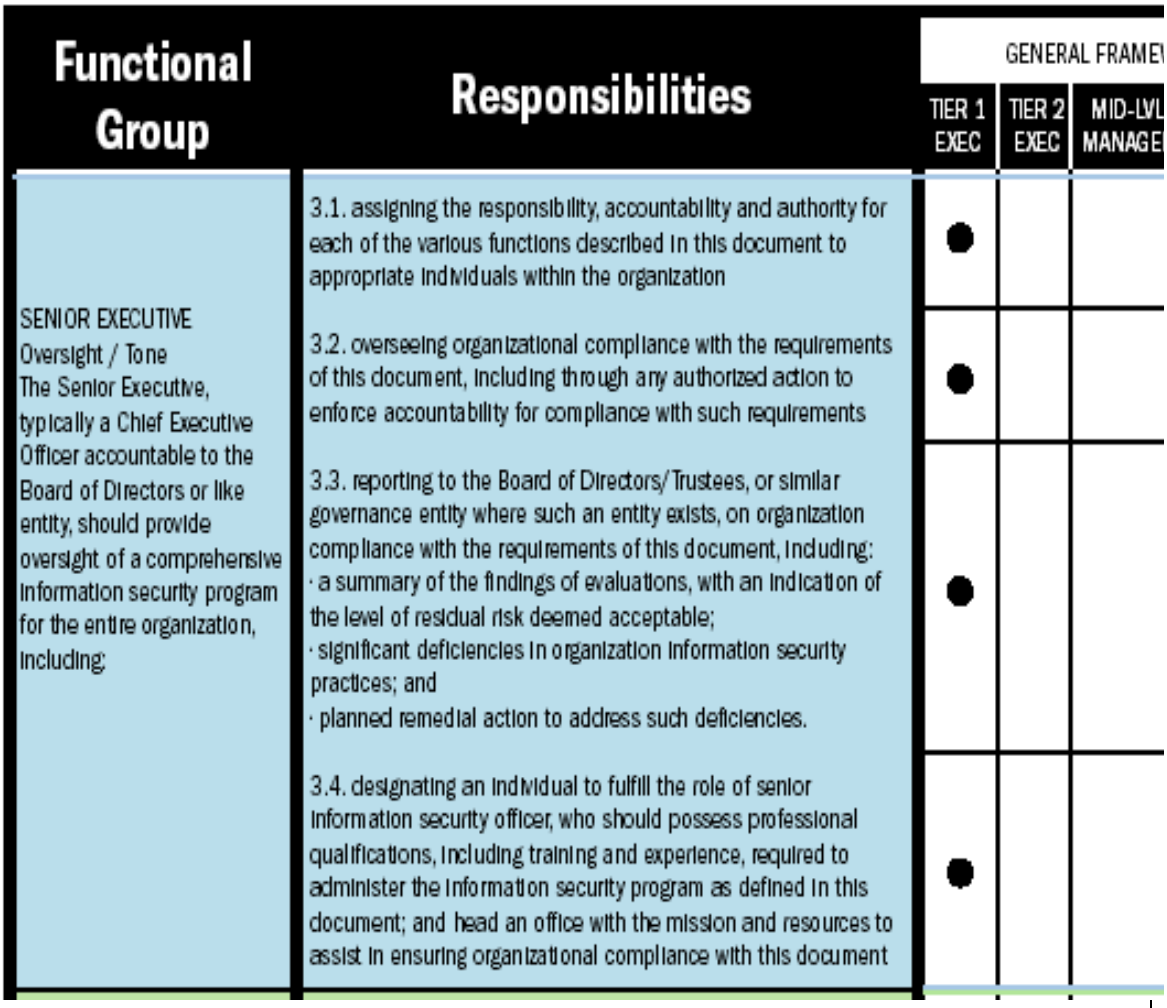
administration and security. The human resource manager's security responsibilities include:

- Implementing and acting in accordance with the company's information security policies.
- Protecting the company's assets from unauthorized access, disclosure, modification, destruction or interference.
- Reacting and helping to resolve security events or security risks reported by employees.
- Ensuring that responsibility is assigned to the individual for actions taken.

The lack of formally defined information security responsibilities in the job descriptions of human resource managers could possibly be due to a lack of use of a structured process and framework for assigning information security responsibilities in many organizations.

An information security responsibility framework would have to have, at least, the following two characteristics. It would have to take into account the multidimensional nature of information security (Von Solms B. , 2001). It would also have to indicate that everyone in an organization contributes to information security. It would have to include responsibilities for all levels of management, including all the parties highlighted in this and the previous chapter.

The framework provided by the Corporate Governance Task Force has both the characteristics described above. It could prove valuable in assisting managers in making information security responsibility more clearly defined for all employees (Corporate Governance Task Force, 2004, pp. 18-19). A small part of the above-mentioned framework is shown in Figure 3.2. This framework is hereafter simply referred to as the information security responsibility framework.



Functional Group	Responsibilities	GENERAL FRAME		
		TIER 1 EXEC	TIER 2 EXEC	MID-LVL MANAGE
SENIOR EXECUTIVE Oversight / Tone The Senior Executive, typically a Chief Executive Officer accountable to the Board of Directors or like entity, should provide oversight of a comprehensive information security program for the entire organization, including:	3.1. assigning the responsibility, accountability and authority for each of the various functions described in this document to appropriate individuals within the organization	●		
	3.2. overseeing organizational compliance with the requirements of this document, including through any authorized action to enforce accountability for compliance with such requirements	●		
	3.3. reporting to the Board of Directors/Trustees, or similar governance entity where such an entity exists, on organization compliance with the requirements of this document, including: · a summary of the findings of evaluations, with an indication of the level of residual risk deemed acceptable; · significant deficiencies in organization information security practices; and · planned remedial action to address such deficiencies.	●		
	3.4. designating an individual to fulfill the role of senior information security officer, who should possess professional qualifications, including training and experience, required to administer the information security program as defined in this document; and head an office with the mission and resources to assist in ensuring organizational compliance with this document	●		

FIGURE 3.2 INFORMATION SECURITY RESPONSIBILITY FRAMEWORK (CORPORATE GOVERNANCE TASK FORCE, 2004, PP. 18-19)

A framework, such as the one provided by the Corporate Governance Task Force, may be used in a formal process to assign information security responsibilities to employees. To illustrate: the following section describes how a set of information security responsibilities for a human resource manager (at the tactical level) can be derived by following a formal process.

The process used below may not be the most effective one. It does, however, illustrate how simply information security responsibilities may be assigned to different employees if a formal process is followed. It is assumed that in organizations where there is no

formal process for assigning information security responsibilities to different individuals, these responsibilities are often not assigned at all.

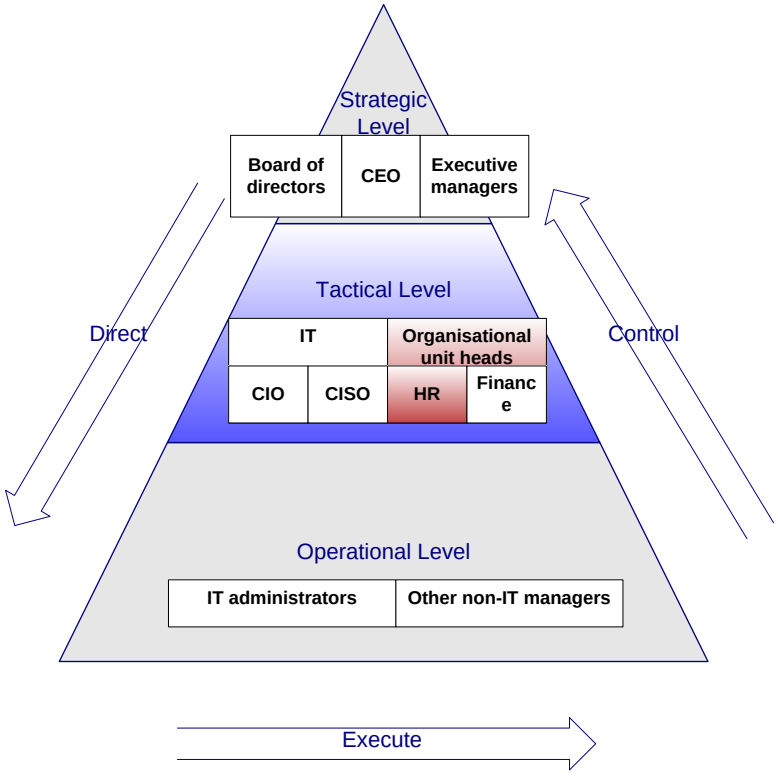
With this in mind, the illustrative process is outlined in Table 3.7 below. The following section then explains how this process can be applied. The process is applied to determining the information security responsibilities of a human resource manager in a specific organization. The process can, however, be similarly applied to any other employee.

Sample process for determining information security responsibilities of employees:
1. Apply the general responsibilities for the appropriate level of management, as shown in the information security responsibility framework, to the employee. 2. Use common practice standards such as ISO/IEC 27002 to find appropriate additional responsibilities. 3. Include a catch-all responsibility. 4. Ensure that defined responsibilities are documented in job descriptions. 5. Ensure that employee receives training and resources needed to discharge these responsibilities.

TABLE 3.6 SAMPLE PROCESS FOR DETERMINING INFORMATION SECURITY RESPONSIBILITIES

3.3.2.3.1 HUMAN RESOURCE MANAGER

This section explains how the abovementioned process for determining information security responsibilities can be applied for a human resource manager in a specific organization.



1. Apply the general responsibilities for the appropriate level of management, as shown in the information security responsibility framework, to the employee.

   The employee is a manager at the tactical level of management. He or she is a head of an organizational unit. According to the information security responsibility framework, the responsibilities outlined in Table 3.5 must, therefore, be considered for this manager. Organizations may choose not to assign every responsibility to the manager; all the general responsibilities should, however, be considered. After considering the general responsibilities for the manager as outlined by the information security responsibility framework, the organization decides to make the human resource manager responsible for the duties shown below.

   - Assess the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of the information and information systems that support the operations and assets under the control of the human resource department.

- Implement policies and procedures that are based on risk assessments and cost-effectively reduce information security risks to an acceptable level.
- Determine the levels of information security appropriate to protect the information and information systems that support the operations and assets under the control of the human resource department. This includes ensuring that the appropriate decisions are made with regard to the sensitivity and criticality of information and identifying user access requirements.
- Periodically test and evaluate information security controls and techniques to see that they are effectively implemented.
- Ensure that the organization has trained personnel sufficient to assist the organization in complying with the requirements of policies, procedures, standards and guidelines provided by the organization.
- See that all employees within the human resource department are aware of their responsibilities to comply with the information security policies, practices and relevant guidance appropriate to their role in the organization.

2. Use common practice standards such as ISO/IEC 27002 to find appropriate additional responsibilities.

   The value of using standards and frameworks such as ISO/IEC 27002 has been shown in the previous chapter. The ISO/IEC 27002 standard has a section devoted to human resource security. Managers may consult this section to find additional duties that the human resource manager may have. As with the previous step, not all the functions listed in this section will apply to the human resource manager. There should, however, be someone in the organization that is responsible for most of the functions. Having a formal process of assigning responsibilities will increase the likelihood that all the necessary duties are performed. After considering the functions listed under the human resource management section of ISO/IEC 27002, the organization decides to, additionally, make the human resource manager responsible for the duties shown below.

- Ensure that employee security roles and responsibilities are defined and documented in accordance with the organization's information security policy.
- Ensure that there is a formal disciplinary process for employees who have committed a security breach.
- Ensure that there is a process in place that ensures all employees surrender all of the organization's assets in their possession upon termination of their employment.

  Ensure that there is a process in place to remove access rights of all employees to information and information systems upon termination of employment.

3. Include a catch-all responsibility.

   In working through ISG frameworks and standards, managers may see the need to assign additional information security tasks to certain employees. A catch-all responsibility such as, "Discharge any additional information security responsibility assigned by appropriate supervisor" can, therefore, be added to the list of information security responsibilities of the human resource manager.

   The final list of typical information security responsibilities for the human resource manager in this organization could, therefore, be similar to the list shown in Table 3.7.

Human resource manager – information security responsibilities:

- Assessing the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of the information and information systems that support the operations and assets under the control of the human resource department.
- Implementing policies and procedures that are based on risk assessments and cost-effectively reduce information security risks to an acceptable level.
- Determining the levels of information security appropriate to protect the information and information systems that support the operations and assets under the control of the human resource department. This includes ensuring that the appropriate decisions are made with regard to the sensitivity and criticality of information and identifying user access requirements.
- Periodically testing and evaluating information security controls and techniques to see that they are effectively implemented.
- Ensuring that the organization has trained personnel sufficient to assist the organization in complying with the requirements of policies, procedures, standards and guidelines provided by the organization.
- Seeing that all employees within the human resource department are aware of their responsibilities to comply with the information security policies, practices and relevant guidance appropriate to their role in the organization.
- Ensuring that employee security roles and responsibilities are defined and documented in accordance with the organization's information security policy.
- Ensuring that there is a formal disciplinary process for employees who have committed a security breach.
- Ensuring that there is a process in place that ensures all employees surrender all of the organization's assets in their possession upon termination of their employment.
- Ensuring that there is a process in place to remove access rights of all employees to information and information systems upon termination of employment.
- Discharging any additional information security responsibility assigned by the appropriate supervisor.

TABLE 3.7 SAMPLE HUMAN RESOURCE MANAGER'S INFORMATION SECURITY RESPONSIBILITIES

4. Ensure that defined responsibilities are documented in job descriptions.

   As has been shown in this chapter, it is important that the information security responsibilities of employees are clearly defined and communicated. Having the information security responsibilities worked into the job descriptions of employees is a means of doing this. The responsibilities of the human resource manager listed above should, therefore, be incorporated into his or her job description. The wording may change and some information security responsibilities may be stated along with other responsibilities. The human resource manager will, however, realize what an important responsibility he or she has to the organization's overall information security programme.

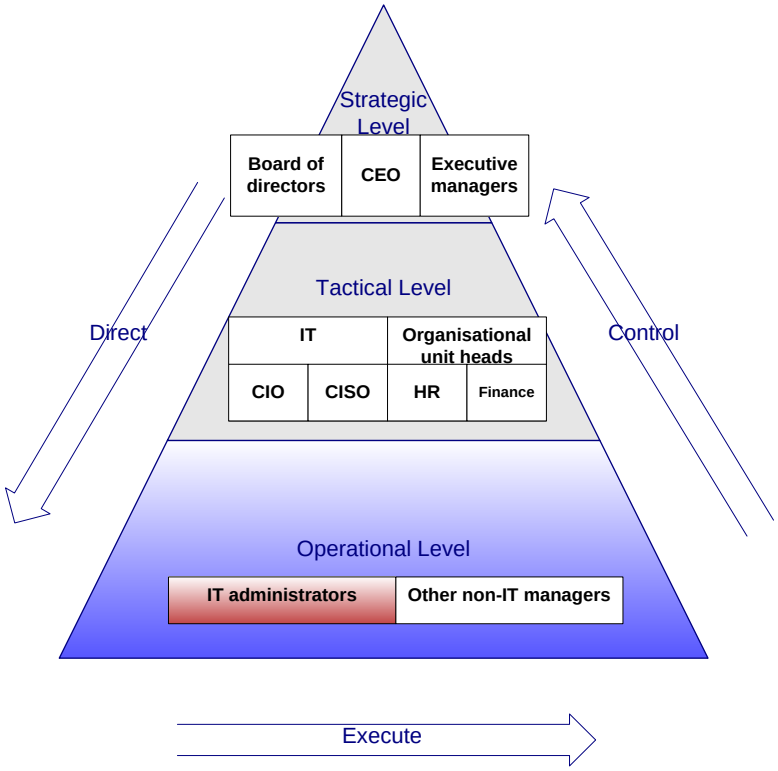
5. Ensure that employee receives training and resources needed to discharge these responsibilities.

   As highlighted in this chapter, non-IT managers should receive support from IT and security professionals in discharging their duties. Each manager should, however, clearly understand what is expected of him or her and how to discharge that duty.

Following a defined, formal process in conjunction with information security responsibility frameworks and information security standards for assigning information security responsibilities makes it relatively easy to make sure that all employees are assigned and made aware of their responsibilities. The process defined above could be applied to other employees as well.

The general information security responsibilities of the operational level of management are considered next.

3.3.3 OPERATIONAL LEVEL



This level of management includes both those who work within the IT unit and those who work with other organizational units. Operational managers within the IT unit typically include system and network administrators. Some of the information security responsibilities of these employees, as compiled by Olivier, are listed in Table 3.7.

As can be seen from Table 3.7, IT administrators play an essential role in making an organization secure. Without the effective actions performed by these employees, the organization would not be secure.

Non-IT staff at this level also contribute to the organization's overall information security status. It is vital that they comply with the information security guidelines and policies provided for them by the managers mentioned previously. The general responsibilities for all employees at this level of management can, actually, be summarized into the three

information security responsibilities set out for all employees in an organization as listed in the next section.

IT administrator – information security responsibilities:

1. *Day-to-day monitoring of the network.*
2. *Functions related to information security services and mechanisms such as identification, authentication, authorization and access control.*
3. *Implementing and executing organizational information security policies and procedures set out by management.*
4. *Administering system and network security for an organization in order to ensure and maintain the required levels of network security.*
5. *Performing upgrades of specific security programs such as virus tools and software patches.*
6. *Administering specific security controls such as backups and access control lists.*
7. *Setting and administering computer policies, system policies and user policies.*

(Olivier, 2006, p. 33)

TABLE 3.8 RESPONSIBILITIES OF IT ADMINISTRATORS (OLIVIER, 2006)

3.3.4 EVERYONE IN THE ORGANIZATION

As has been emphasized numerous times in this and the previous chapter, everyone in an organization has a role to play with regard to information security. This includes the managers already addressed above and any other employee in the organization. Everyone in the organization has at least three very important information security responsibilities.

1. Be aware of and understand their personal information security responsibilities (ITGI, 2007, p. 25; Corporate Governance Task Force, 2004, p. 14). For most users, this can be done by maintaining knowledge of the company's ever changing information security policies, standards, guidelines and procedures. Users should also make sure they understand any information security responsibilities outlined for them in their individual job descriptions.

2. Comply with all the information security responsibilities assigned to them by the organization (ITGI, 2007, p. 25; Corporate Governance Task Force, 2004, p. 14). This would mean complying with all requirements described in the above mentioned documents. This would typically include, at least, things such as having secure passwords and disposing of sensitive information in an appropriate manner.
3. Report any information security vulnerabilities or incidents in the appropriate way (Corporate Governance Task Force, 2004, p. 15; ITGI, 2007, p. 25).

3.4 CONCLUSION

The information security responsibilities of various managers involved with ensuring effective information security have been considered. The importance of having the information security roles and responsibilities of all employees clearly defined and communicated has been made clear. Even though the importance of having clearly defined information security responsibilities outlined in job descriptions, a search of job descriptions for human resource managers showed that they generally do not have information security mentioned in them. It has been illustrated how easily the information security responsibilities for employees can be identified by using a formal process in conjunction with an information security responsibility framework and ISG best practice standards.

In considering the responsibility of the various managers, the value that an automated tool which facilitates the provision of management information for ISG would add becomes apparent. At the strategic level, both the board and CEO have responsibilities with regard to information security reporting. The board has the responsibility to require meaningful and regular information security reports. CEOs have the responsibility to develop and introduce clear and regular reporting on the organization's information security status to the board. At the tactical level of management, managers would also benefit from a configurable tool that would provide the appropriate information security information to different individuals. IT managers such as the CIO and CISO would benefit from a tool that provides a holistic view of information security and allows them

to get detailed information on any problem that they would then be responsible for. A tool would also assist the CIO and CISO to do their duty of providing strategic managers, like the board, CEO and organizational unit heads, with the relevant meaningful information security information that will help these managers to discharge their information security responsibilities. Similarly, all other employees, including non-IT managers at the tactical level, would benefit from such a tool since it could provide them with information security information that would help them discharge their information security responsibilities.

Some of the characteristics of such a tool also become apparent when discussing the responsibilities of those who would make use of it. As has been mentioned, the tool will have to be configurable to meet the needs of different users. It has been shown that different users would need different information security information. It has been shown, for example, that organizational unit heads would need information that would assist them in discharging their information security responsibilities within that unit. Board members would, on the other hand, benefit from reports showing the effectiveness and deficiencies of the information security programme. As highlighted in this chapter, the reports they receive should show areas of risk and the status of the security programmes related to these areas. To be able to give such a holistic view of the information security programme, the tool will also have to be able to collect and process a wide variety of types of information security information. This chapter also pointed out that everyone in an organization, including the board and executive management, has to have an understanding of what is acceptable with regards to information security areas and what the company finds unacceptable. A tool that shows the state of security areas as related to accepted thresholds could, therefore, be of value.

Many information security reporting tools are available. Some of these tools and their ability to provide the functionality needed by the managers discussed above are discussed in the next chapter.

Information Security Reporting Tools

Chapter 4

INFORMATION SECURITY REPORTING TOOLS

4.1 INTRODUCTION

The preceding chapters have highlighted the important role that people and processes play in ensuring effective information security. No organization will, however, be secure if the necessary technical controls have not been implemented (Grance, Stevens, & Myers, 2003, pp. 1, 6). There are scores of tools available that are used to assist in effective information security. Most of these tools make information security data available. To illustrate, anti-virus tools not only protect a network against viruses but also make information available about the number and type of viruses detected on the network. The previous chapter mentioned that an automated means of providing relevant information security information to all employees would be valuable. The purpose of this chapter is to highlight that there is still a need for tools that make appropriate information security information available in a meaningful manner to various managers, including organizational unit heads, in a manner that smaller organizations with few resources would be able to benefit from. This will be done by discussing existing information security tools.

There have been, and will continue to be, marked advances in information security tools and technologies. A trend with regard to information security tools recently has been a progression from single-purpose information security tools to SIM (security information management) suites (Mitropoulos, Patsos, & Doulgigeris, 2007, p. 227). SIM applications have themselves changed over the years from tools that are used by security officers primarily to identify and handle security events to tools that are also used to show compliance (Shipley, 2006). In the last couple of years, SIMs have evolved to be of use to non-IT managers in organizations as well. SIMs are described in more detail later in this chapter. Tools from each phase of this progression from single-purpose information security tools to SIMs are discussed in this chapter. As will be seen from the description of tools used in each phase, SIM tools do not replace single-purpose security tools. Each still makes a valuable contribution to the management of information security.

4.2 SINGLE-PURPOSE INFORMATION SECURITY TOOLS

A plethora of information security tools, clearly designed for use by operational IT and information security staff, exist. These tools often provide a means for implementing some type of information security control: for example, an antivirus tool used to detect and remove viruses on the network or a firewall system to control network traffic to and from an internal network. Besides accomplishing such specific information security tasks, these tools often collect and report on valuable information security information. Many other network monitoring tools are commonly used by IT and information security staff to assist them in accomplishing their information security duties. These tools also collect valuable information that helps establish how secure an organization is. To illustrate this, some popular tools used by information security staff are described below.

4.2.1 NMAP

Nmap is a tool that is often used in performing security audits. It provides information about a network such as which operating systems are being run, what services are being provided and the types of firewalls/filters that are in use (insecure.org, 2005). This type of information plays a vital role in assisting information security professionals to analyse the security of a network. Figure 4.1 depicts the typical format of the output generated by running Nmap. Although the value of this type of information for an information security professional is unquestionable, it should be clear that a report such as the one depicted in Figure 4.1 would be of little value for any non-IT employee in the organization.

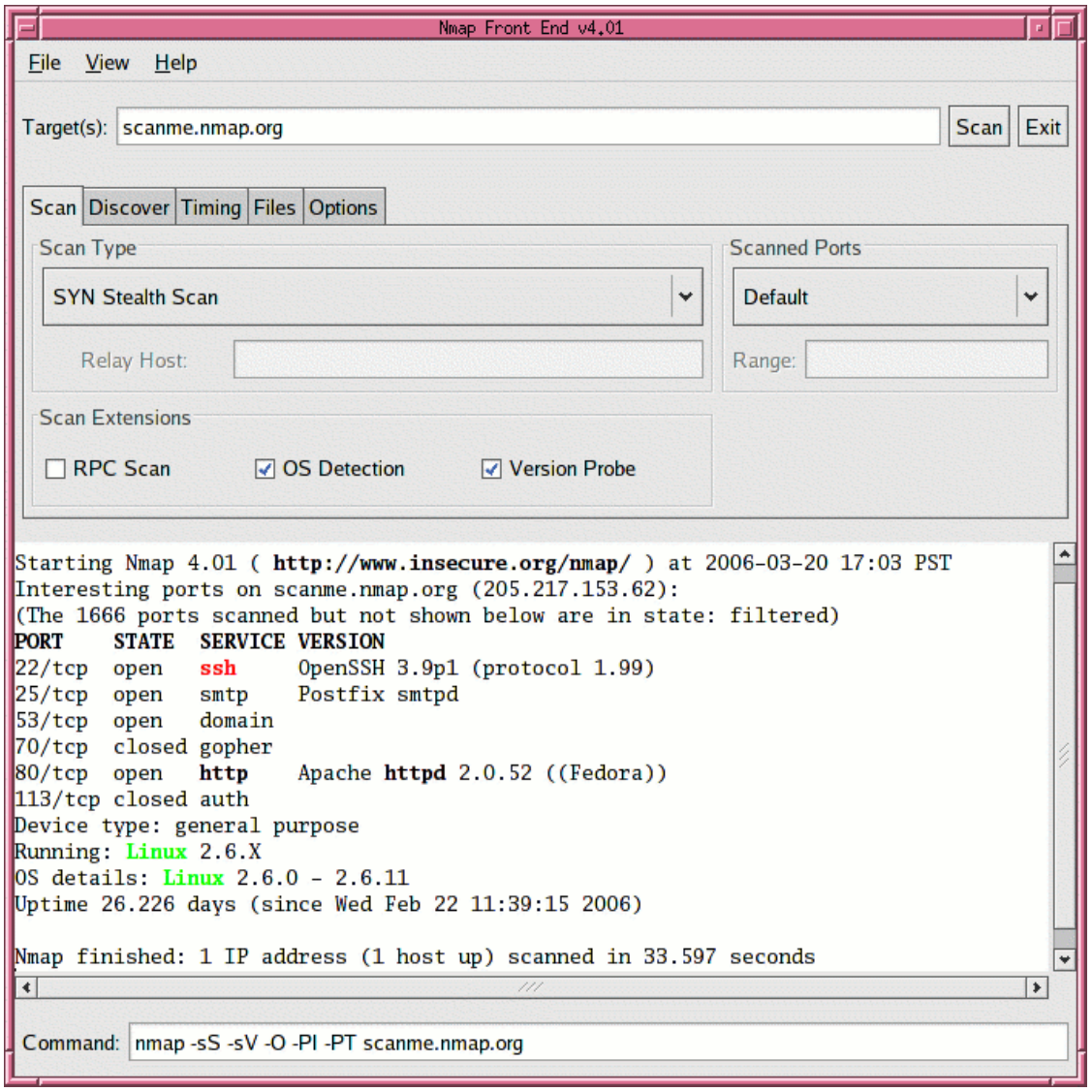


FIGURE 4.1 NMAP SCREEN (INSECURE.ORG, 2006)

4.2.2 SNORT

Snort is an extremely popular tool among information security professionals. It is "the most widely deployed intrusion detection and prevention technology worldwide and has become the *de facto* standard for the industry" (Snort.org, 2008). It has received SC Magazine's 2008 award in the Best Network Security category (SC Staff, 2008). Snort is also a free, open-source tool. It has been listed as one of the ten best free security tools available on the IT security web site by John Edwards (Edwards, 2008). Besides acting as

a full intrusion detection and prevention system, it can also be used as a straight packet sniffer or packet logger. It analyses network traffic and can detect a variety of attacks including stealth port scans, CGI attacks and operating system fingerprinting attempts (Snort.org, 2008). Snort can be configured to store the information it collects in various places such as the SQL databases, the syslog facility and UNIX domain sockets (The Snort Project, 2008, pp. 79-83). Snort can also be configured to provide real-time alerts. Information security professionals will have to ensure that they receive, analyze and act based on the information provided by this tool so as to be able to protect the network from intrusions. Snort is often used in conjunction with tools such as Basic Analysis and Security Engine, BASE. BASE is a tool that processes databases that contain information such as that collected by SNORT and displays the information in a web front end. The information can hereby be shown in a more user friendly manner (Rich, 2005). Samples of reports generated by BASE from information collected by SNORT are shown in Figures 4.2 and 4.3.

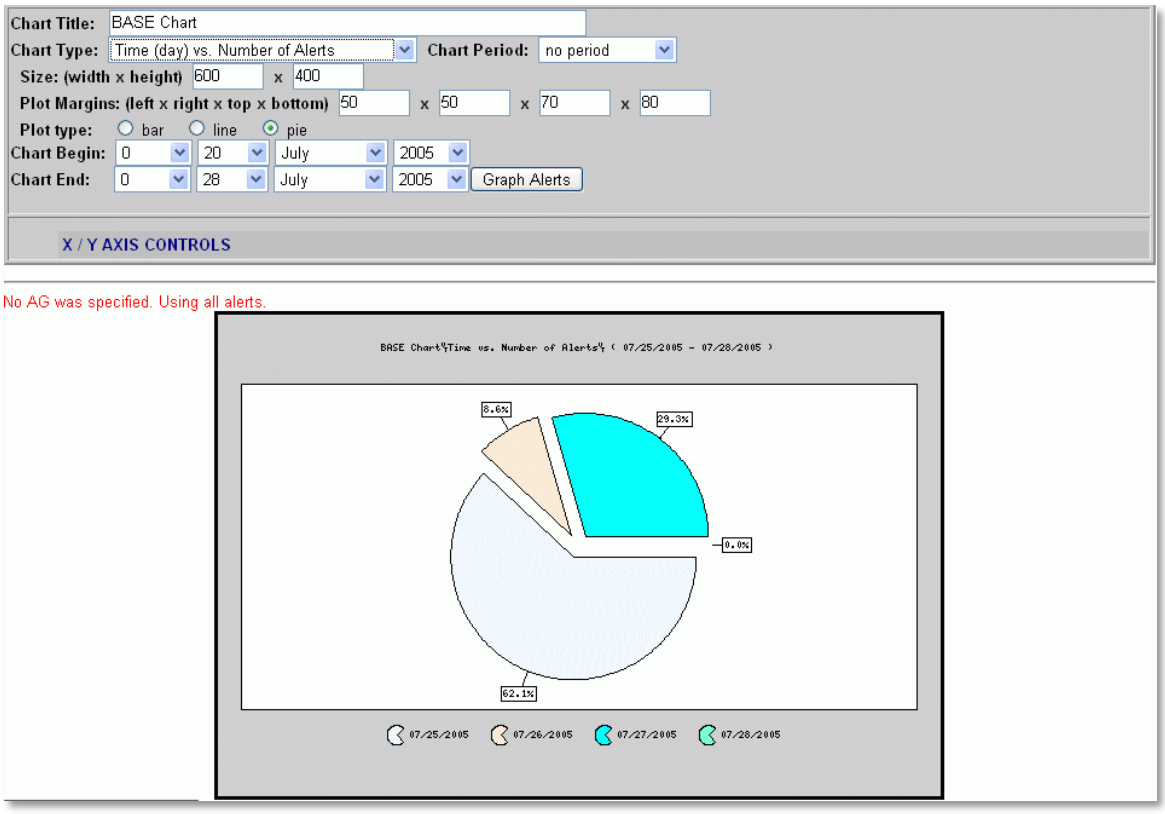


FIGURE 4.2 BASE CHART SHOWING NUMBER OF ALERTS AT SPECIFIC TIME OF DAY (RICH, 2005)

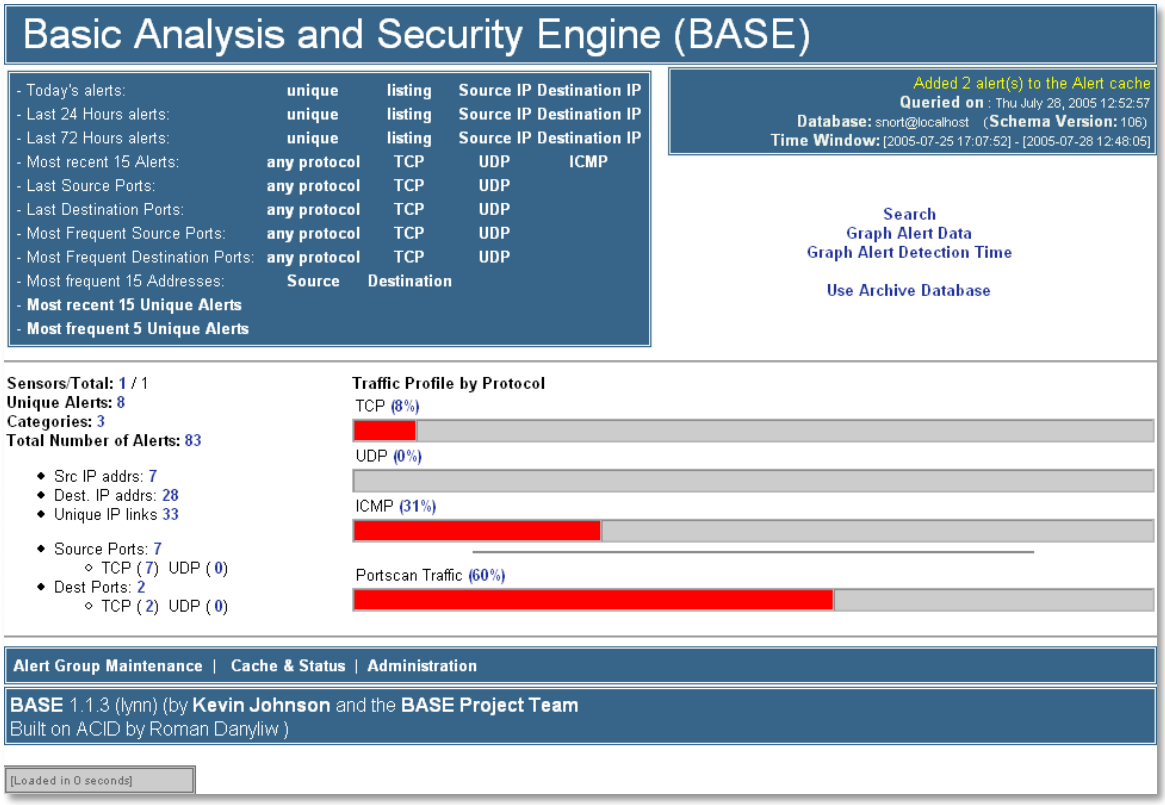


FIGURE 4.3 MAIN PAGE OF BASE (RICH, 2005)

As can be seen from the above description of SNORT and a sample of the reports generated from SNORT information by BASE, it should be clear that these tools are not designed for use by non-IT managers at either strategic or tactical levels of management. Although the information collected and reported on by these tools is extremely valuable in assisting information security professionals with technical knowledge to accomplish information security, it can be argued that it would be of little value to non-IT employees.

4.2.3 NESSUS 3

Nessus is another very popular information security tool. It is a free vulnerability scanner. Nessus 3 was a finalist in SC Magazine's Reader Trust Award in the category "Best Audit/Vulnerability assessment solution." It was also featured in the December 2007 issue of SC Magazine as one of the best products of 2007. In October 2007, it won the

WindowSecurity.com Readers Choice Award in the Security Scanner Software category (Tenable Network security, 2008).

Nessus scans devices on a network to identify security vulnerabilities. From the information collected during the scan, Nessus reports on identified vulnerabilities. An example of such a report is shown in Figure 4.4 below. The tool also provides vulnerability recommendations and the ability to track remediation and audit security patches (Tenable Network security, 2008).

It should, once again, be apparent that although the information provided by this tool is critically necessary in being able to ultimately provide high levels of information security, the tool is designed for use by IT and information security professionals, not non-IT staff.

FIGURE 4.4 NESSUS VULNERABILITY REPORT

The above mentioned tools are just three of scores of tools commonly used to contribute to the security of an organization's information. To demonstrate how many information

security tools are available, consider the following. The SC Magazine Awards are designed "to reward excellence and innovation in the IT security industry" (SC Magazine, 2008). According to Tenable Network Security, there were over 600 entries in over 30 technology categories (SC Magazine, 2008).

The NIST special publication 800-36 provides nine IT security product categories (Grance, Stevens, & Myers, 2003, p. v). Eight of these categories and some of the tools that provide information security information and are designed for use by IT and information security staff are listed in Table 4.1.

These tools play an absolutely vital role in ensuring information security. The popularity and effectiveness of these tools leaves no question as to the value that they have to information security professionals. The information that they collectively provide assists information security professionals to make an evaluation of how well their organization's information security is being taken care of from a technical perspective. Based on this information, these employees act to make the organization's information more secure. Everyone, therefore, benefits from the information provided by these tools. When considering the type of information these tools provide individually, though, it can be argued that they are not designed for use by non-IT organizational unit heads, the board, the CEO or other non-IT employees. The reports provided by these tools alone would be largely meaningless to these managers.

Information security professionals at the tactical level of management, such as the CISO and CIO, play an important role in the management of the entire security programme. These managers must, therefore, be aware of the state of each information security concern as well as how well the overall information security program is being implemented. These managers, therefore, have the daunting task of making sense of the information security information that they receive from a variety of sources about a variety of information security concerns (Shipley, 2006). It should be clear that managers concerned with ISG would benefit from a central store of information security information that can be analyzed to show the state of an organization's information security. With regard to this, Shipley states, "Automation becomes critical when reviewing logs from more than a few devices, and SIM products with correlation and

event-reduction capabilities can really help here" (Shipley, 2006). It can, therefore, be argued that it is important to integrate information and reporting mechnisms provided by these various tools.

IT security product category	IT security product
Identification and Authentication	• Hitachi ID management suite (Hitachi ID Systems, 2008)
Access Control	• Safe Access (StillSecure, 2008)
Intrusion Detection	• Snort (Snort.org, 2008) • IPS 5500-150Ev5.12 (Top Layer Security, 2008)
Firewall	• Corporation Sidewinder 7.0 (Secure Computing Corporation, 2008)
Public Key Infrastructure	• PlexCrypt (PlexObject Solutions, 2006)
Malicious Code Protection	• Enterprise management (Savant Protection, 2007) • Interscan Gateway Appliance (Trend Micro, 2008)
Vulnerability Scanners	• Tenable Nessus 3 (Tenable Network security, 2008) • NeXpose (Rapid 7, 2008)
Forensics	• ProDiscover IR v 4.9 (Technology Pathways, 2008) • LiveWire Investigator v.3.1.1c (Wetstone Technologies, 2008)

TABLE 4.1 NIST IT SECURITY PRODUCT CATEGORIES AND EXAMPLES

The following section describes some security information management (SIM) tools that have proved valuable in assisting IT managers who need a holistic view of information security concerns. A brief description and history of SIMS is, however, first provided.

4.3 SECURITY INFORMATION MANAGEMENT TOOLS

Security Information Management (SIM) tools have become popular in recent years. It is believed that the influence that they will exert over companies of all sizes, worldwide, will increase substantially in the coming years. This is brought to the fore strikingly in a report by Gartner Dataquest (Bussiness Wire, 2008). According to an article in Business Wire, the report states that overall spending on SIM technologies will have a compounded annual growth rate of 19.3% based on revenue through 2012 (Business Wire, 2008). Dubie similarly mentions a Forrester Research report which shows that the market for SIMs will continue to grow at about a 50% rate until 2009 (Dubie, 2008). This Forrester Research report further highlights the key role that these technologies will play in contributing to ISG. According to Dubie, part of the report reads, "SIM will be the *primary tool* for enabling operations teams and security teams to collaborate on: turning business policy into specific configurations and requirements; assessing the risk of ongoing security issues; and coordinating the response to security incidents". From the above, the clear importance of SIM technologies should be apparent. What, though, are SIMs?

Security Information Management (SIM) tools are also referred to as SEM (Security Event Management), SIEM (Security Information and Event Management) or ESM (Enterprise Security Management) tools (Kim, Kim, & Lee, 2006, p. 228; Shipley, 2006; Mitropoulos, Patsos, & Doulgigeris, 2007). Simply put, these are tools that report on information security data collected from a number of sources. To do this efficiently, these tools typically collect, normalize, aggregate, correlate and archive information security data from various data stores (typically log files). They then also visualize this combined information in a meaningful way (Mitropoulos, Patsos, & Doulgigeris, 2007, pp. 228-230; Shipley, 2006). This chapter has previously touched on the need for this type of solution. It has been highlighted that those who are responsible for information security need a way to analyse security information from various sources. With the vast amount of information security made available by various tools today, automation becomes necessary in meaningfully correlating the available information. NetForensics summarises why SIMs are necessary as follows; "Your security management solution is

only as good as the breadth and availability of the underlying data. Yet relevant security data are dispersed across your organization, and without the right structure to monitor, correlate, and analyze your data, mitigating security threats and ensuring compliance is virtually impossible" (netForensics, 2007).

SIM tools are relatively new tools used in ensuring information security. This is illustrated by work done by Greg Shipley from the Network Computing Magazine over several years (Shipley, 2006). Shipley reports on an initial review of SIM products available in 2002. The tools that where available then were described as "immature" (Shipley, 2006) and difficult to configure but with the potential to add value (Shipley, 2002, p. 51). In a similar review in 2006, Shipley had the following to conclude about the available SIM products, "Saying the market is in disarray is an understatement. We've covered SIMs for years, and our heads are spinning. Pity the typical customer" (Shipley, 2006). In 2005, Messmer attributed the slow adoption of such tools to very high costs but once again emphasized that the companies using them found them invaluable for their information security managers (Messmer, 2005). Although still referred to as an emerging technology in 2007 (Mitropoulos, Patsos, & Doulgigeris, 2007, p. 227), SIMs have improved significantly and are currently effectively used by a number of organizations.

Initially, most SIMs were geared for use by information security professionals at the operational level (Dubie, 2008a). Some SIMs available for use by these managers are described below.

4.3.1 SIMs FOR IT AND INFORMATION SECURITY PROFESSIONALS

The tools discussed in this section make information security information available in a manner that would most likely be valuable to IT knowledgeable managers at the tactical level of management. They are not geared for use by non-IT managers, as is shown below in the description of the information these tools make available.

4.3.1.1 TRIGEO SIM

Trigeo SIM is an appliance that can be installed and easily configured for use in medium to large organizations. This appliance not only acts as an IPS/IDS, it also logs the event every time USB storage devices are plugged into any device on the network. In addition, Trigeo SIM integrates with various network infrastructure components from firewalls to anti-viruses. This tool performs real-time log-analysis and has prebuilt correlations. From the information gathered by this tool, various security event and activity reports are generated. As can be seen from the figures below showing sample reports, the reports show the security event information in an easy-to-understand graphic format. The tool can produce over 250 stock reports. Although the tool is specifically aimed at IT professionals, the marketers do claim that it can generate reports in "multiple formats to provide a picture of security of both technical staff and non-technical management" (TriGeo Network Security, 2007).

Trigeo has been recognized as a superior product. The SC Magazine awarded this product five stars and ranked it as a 'best buy' product (Stephenson, 2006). Trigeo SIM was also a leader in the Gartner magic quadrant for SIEM in 2007 (Trigeo, 2007).

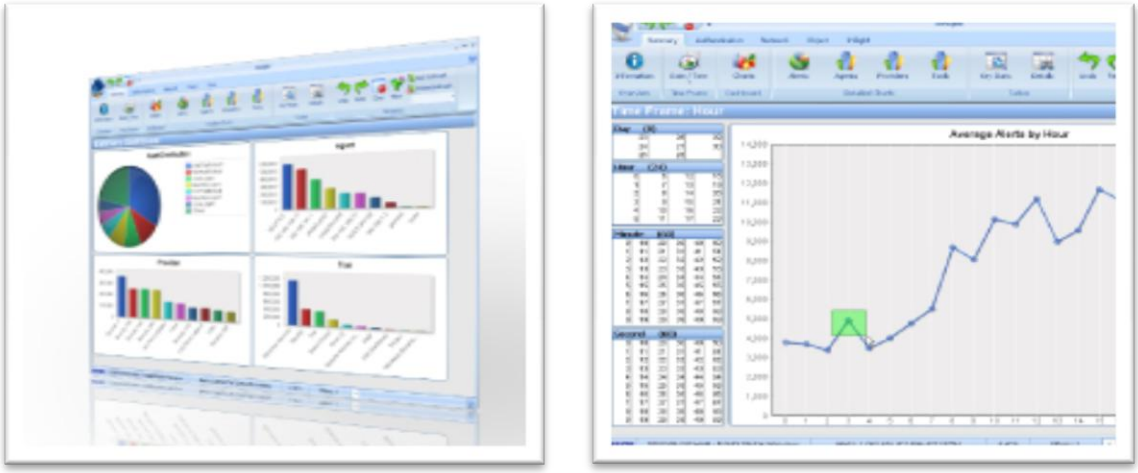


FIGURE 4.5 SAMPLE TRIGEO REPORTS (TRIGEO NETWORK SECURITY, 2007)

4.3.1.2 THE SOURCEFIRE 3D SYSTEM

On the official website for this product, the limitations of single-purpose information security products are highlighted. Sourcefire then describes the 3D system as "the first and only Enterprise Threat Management (ETM) solution that unifies IPS, NBA, NAC and vulnerability assessment technologies…" (SourceFire, 2008). The system is named 3D because of the discover, determine, defend approach that is followed. Information security information is collected or discovered using, amongst other things, the SNORT vulnerability-based detection engine. The information is then correlated and analyzed to determine "policy violations, the impact of security events and the appropriate response" (SourceFire, 2008). The system also allows users to defend the company's information security by addressing known vulnerabilities and blocking attacks as they occur. The interface where the meaningful information is presented is described as "a web-based GUI which just gets it right".

4.3.1.3 SECURITY OFFICER'S BEST FRIEND (SOBF)

The SOBF is a tool that is made freely available by the Security Officers Management and Analysis Project (SOMAP). The aim of this organization is to provide open-source information security risk management tools and utilities (SOMAP.org, 2007). The SOBF tool is "an information security governance, risk and compliance tool which can be used for gap analysis, risk analysis and as a general IT security management tool" (SOMAP.org, 2007). The tool is still in very new and will still require a great deal of work from contributors to the project. McRee, however, concludes about the project, "This is a great start on a project with great potential, focused on a discipline in its ascension to its rightful place in the larger framework of information assurance". McRee describes the tool's three phases: context establishment, risk retention and risk treatment. In context establishment, you get data about your organization by conducting an asset inventory, conducting a threat analysis or conducting a vulnerability analysis. In the risk retention phase, risk identification, estimation and evaluation is done. During the final phase, controls which offer mitigation safeguards are shown (McRee, 2007). Although this tool can still be enhanced, the framework used and the extensible toolset approach followed by the developers makes this a project with great potential (SOMAP.org, 2007).

4.3.2 SIMS FOR MANAGERS

The fact that staff other than IT and information security professionals have information security duties and would, therefore, benefit from appropriate information security information has been highlighted in previous chapters. Dubie shows how the SIM industry has recognized this fact by quoting Paul Stamp, a principal analyst who contributed to the Forrester Research report mentioned earlier, as having said, "[SIM] tools used to be purely the domain of the security analyst working on operational issues. These days, the information that a [SIM] tool provides often ends up on the CISOs, or even the CIO's, desk" (Dubie, 2008a). Two of the leading SIM tools that can make information security information available to non-IT managers are described below.

4.3.2.1 NFX SIM ONE

nFX One is a product made available by a pioneer of the SIM market, netForensics (Compliance Home, 2007). Like all other SIMs, the tools collect, analyse and report on an organization's information security information. Whereas the SIMs mentioned previously have collected information mainly from security devices, nFX One collects information from monitored applications and databases as well as from security and network devices and scanners (netForensics, 2007). The tool also uses "multi-dimensional correlation technology" and conducts rules-based, vulnerability, statistical and historical correlation (netForensics, 2007). The tool also provides the "gold standard for enterprise reporting" by making use of crystal reports. Not only does the tool provide a powerful and easy to use GUI that users can use to access information, it also has the ability to generate meaningful reports and provides various dashboards. The tool allows security teams to generate their own custom reports and provides prepackaged report templates for analysts, operators and executives. The executive reports and dashboards show "overall security posture, vulnerability, and incident management trends" (netForensics, 2007, p. 3). There are also executive reports available that show compliance with regulations like PCI, FISMA and HIPAA. This is obviously a very powerful tool that has the ability to contribute greatly to ISG. A sample report from this product is shown in Figures 4.6.

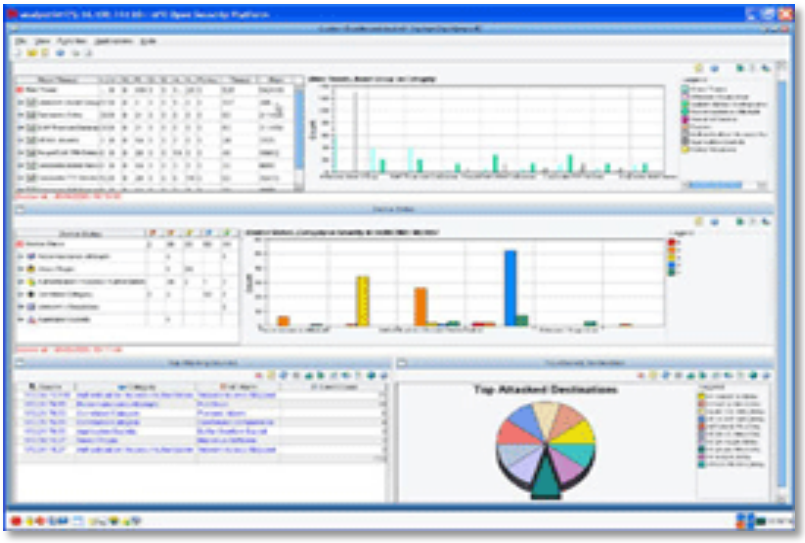


FIGURE 4.6 SAMPLE NFX SIM ONE REPORT (NETFORENSICS, 2007)

4.3.2.2 INTELLITACTICS SIEM

Intellitactics is another very popular SIM. It has won the SC Magazine 2008 award in the category Best Security Management (SC Staff, 2008). The Department of Justice Executive Office for United States Attorneys (EOUSA) has recently chosen to use products from the Intellitactics SIEM suite extensively as part of its enterprise security management system. (KM World, 2007)

Intellitactics SIEM stores the information security data collected in a data warehouse. The data in the warehouse is analyzed and reported on using Intellitactics SAM. Intellitactics SAM includes a dashboard template library and a library of security assurance metrics (therefore, SAM). Each dashboard template can be configured with metrics that are dynamically updated to provide the relevant information. In this way, organizations can use this tool to make relevant information security information available to various employees. According to Business Wire, this product allows users to move easily "between enterprise view and specific business unit or physical location views; between summary and detail" (Business Wire, 2005). It should be clear from this brief description that this product contributes significantly to ISG by allowing all ISG

role-players to receive relevant information security information. Figure 4.7 below illustrates a sample Intellitactics dashboard.

FIGURE 4.7 SAMPLE INTELLITACTICS SAM DASHBOARD (INTELLITACTICS, 2007)

4.4 CONCLUSION

As can be seen from the above discussion, it is clear that the security tool market has, and will continue, to make significant adjustments to meet the needs of organizations which all have the responsibility of ensuring information security. The market has evolved from providing only single-purpose security tools to SIM tools that put together information security information and functionality typically provided by several of these single-purpose tools. The SIM market itself has evolved over the years. One trend in the SIM market has already been shown in this chapter. Initially, SIMs were designed for use by operational information security professionals. Today, however, some SIMs are being used to present the relevant information security information not only to these users but also to information security professionals at the tactical level of management, executives and other non-IT managers.

Compliance requirements have also had a marked impact on SIMs (Shipley, 2006; Carr, 2007). Instead of simply showing information derived from the analysis of correlated information collected from perimeter security devices, SIM tools have increasingly been used to show compliance to company policies and regulations like PCI, FISMA and HIPAA.

Smaller organizations with fewer resources can often realistically simply not afford to take care of information security in the same manner as bigger organizations (Ross, 2008, p. 9). It is, therefore, fitting that a key trend in the SIM market at the moment is the shift from expensive and complicated SIMs for big enterprises to the development of SIMs for smaller companies that do not have the resources to make the use of many of the SIMs discussed in this chapter viable (Carr, 2007). Dubie highlights how the Forrester Research report shows how this trend is, in fact, one of the factors that will drive the growth in the SIM market in the coming years. Dubie shows that the Forrester Research report predicts that although small companies (fewer than 1000 employees) currently only make up about 1% of the SIM market, they could make up about 30% by 2011 (Dubie, 2008a).

There is, therefore, still a need for an affordable way of making information security information visible to all managers in smaller organizations that do not have the resources required by the commercial SIMs like Intellitactics that provide this facility.

FISMI DESIRABLE CHARACTERISTICS

Chapter 5

FISMI DESIRABLE CHARACTERISTICS

5.1 INTRODUCTION

This chapter provides a list of the characteristics that would be desirable in a framework (FISMI) that makes information security information visible to managers throughout an organization. The list has been compiled by studying characteristics of Security Information Management tools (SIMs), management information systems (MISs), decision support systems (DSSs), executive dashboards, compliance dashboards and continuous auditing tools.

How SIMs contribute to information security visibility throughout an organization has already been discussed. It should, therefore, be clear that a study of what makes these tools effective will contribute to an understanding of the desirable characteristics of the above-mentioned framework. The following section will briefly define the other systems listed above and motivate how they are related to a framework that will facilitate the visualization of collated information security management information to all levels of management to support ISG. The desirable characteristics for such a framework are then listed and motivated.

5.2 CONTINUOUS AUDITING TOOLS AND MODELS

Continuous auditing is defined as "a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short time after, the occurrence of events underlying the subject matter" (Chartered Accountants of Canada, 1999). Information technology plays an essential role in making continuous auditing possible (Searcy & Woodroof, 2003, p. 46; O'Reilly, 2006).

There are several benefits associated with continuous auditing as opposed to traditional scheduled audits. Some of the benefits that O'Reilly highlights are quoted below.

- Continuous auditing can make the audit process faster, cheaper, and more effective.
- Using IT also makes it possible for auditors to test entire populations of data instead of simply testing data samples.
- It provides the means "for internal audit to strengthen reporting to and communication with senior management and the audit committee".
- "It strengthens the ability of internal audit to communicate more effectively with business units" (O'Reilly, 2006).

Company's acceptance of continuous auditing testifies to its practical value. Meg Green reports that the Pricewaterhousecooper's 2006 State of the International Audit Profession study showed that 81% of the companies it had surveyed either already had continuous auditing or continuous monitoring in place or were planning on implementing it (Green, 2006, p. 76).

Although continuous auditing refers primarily to the auditing of financial matters, many of the principles learnt from continuous auditing can be applied to information security auditing and visibility. In Chapter 3, it was highlighted that audit committees are becoming increasingly responsible for non-financial aspects of business such as information security audits. Since auditors benefit from continuous auditing for financial matters, will they not also benefit from continuous auditing of information security? Since the value of using IT in continuously auditing financial matters has been widely recognized, should it not be even more apparent that IT should be used to continuously audit information security matters? Furthermore, technology-based continuous auditing of information security could potentially result in all the same benefits listed above for continuous auditing of financial matters. Some of these benefits are, in fact, the same as the goals of the framework that is to be developed. The framework will be used to strengthen reporting to and communication with senior management and the audit committee about information security. It will also enable the more effective communication between business units about information security concerns. Continuous

auditing enables the provision of 'evergreen' financial reports. "Evergreen reports are audited reports available whenever a user accesses a web page within the continuous auditing environment. The reports are dynamic to the time the user accesses the site" (Flowerday, Blundell, & Von Solms, 2006, p. 326). In a similar way, one of the main objectives of this work is to develop a framework that will facilitate the visualization of collated information security management information to all levels of management to support ISG. The framework should, in a sense, make the appropriate evergreen information security reports available to all ISG stakeholders.

Reflecting on the comparisons that can be made between the goals of FISMI and those of continuous auditing tools, it should be clear why continuous auditing tools and models have been studied to discover the desirable characteristics of a framework that will facilitate the visualization of collated information security management information to all levels of management to support ISG.

5.3 MANAGEMENT INFORMATION SYSTEMS (MISS)

A Management Information System (MIS) is "an information system that makes information available to support managerial decision making. It produces displays and reports on a periodic, exception, or demand basis" (O'Brien, 1999, p. 61). There are various types of MISs, such as Decision Support Systems (DSSs) and Executive Information Systems (EISs).

"A decision support system is a system under the control of one or more decision makers that assists in the activity of decision making by providing an organized set of tools intended to impose structure on portions of the decision-making situation and to improve the ultimate effectiveness of the decision outcome" (Marakas, 2003, p. 4).

An EIS "is a special type of DSS designed to support the decision-making process of managers at the strategic level of management" (Marakas, 2003, p. 174).

Managers from various fields, such as health management, construction management and human resource management, make use of MISs. These systems have proved to be

effective in assisting managers to carry out their management roles. It has been made clear in previous chapters that information security management is also an important responsibility for managers throughout an organization. It, therefore, follows that a MIS for information security would also prove helpful.

5.4 EXECUTIVE DASHBOARDS AND COMPLIANCE DASHBOARDS

Dashboards are tools that are used by managers to show them, at a glance, how they are performing (Robertson & Raddeman, 2004). According to Sardoni, they are typically used to answer questions such as: What do I need to follow up on today? How well are we doing? What is holding us up from achieving our goals? How far are we progressing? (Sardoni, 2002, p. 15) Like dashboards, a FISMI should also act as an enabler to help managers answer questions like those mentioned above with regard to information security.

The outstanding strength of dashboards is their effective way of making the necessary information visible in an easy-to-understand manner. The principles and techniques they use to achieve this are to be used in the design of a framework for information security reporting.

It should be clear from the preceding sections that there are similarities between FISMI and continuous auditing systems, MISs and dashboards. Many of the characteristics that make these tools popular and desirable should, therefore, also be desirable characteristics of FISMI.

Some of these desirable characteristics are discussed in the following section.

5.5 DESIRABLE CHARACTERISTICS

The previous chapter highlighted the need for more affordable tools that can be used to assist various managers with their ISG responsibilities. Existing tools, such as some of the SIMs mentioned, which are effective in assisting managers in this regard are expensive. One of the desirable characteristics for a FISMI is, therefore, affordability.

1. **Affordability.** A framework for information security visibility should be affordable. Smaller organizations with fewer resources should also be able to benefit from applications implemented based on the FISMI.

When discussing information security reporting, it is important to understand the extremely dynamic nature of the information security in any organization (Karygiannis, 2008; Swanson & Guttman, 1996, p. 9; Grance, Stevens, & Myers, 2003). The IT environment itself constantly changes. New technologies are developed. The value and use of information in organizations change. The network and IT infrastructure that support the company may change and expand. In addition to this, there are constantly new threats, vulnerabilities and risks that can affect organizations and new ways to respond to these. When taking the above into account, it becomes clear that a framework for information security visibility must allow for flexibility. The framework will have to support:

2. **Scalability.** Scalability is "the capability of hardware or software to accommodate increasing numbers of users" (Pfaffenberger, 1997, p. 457). FISMI will have to be able to accommodate organizations of various sizes. It will also have to be able to cope with growing organizations. FISMI must support organizations with either small or large networks and many or few users. It should also allow the administrators to determine how much and what kind of information security data they want to collect (Dubie, 2008). Advances in technology will also undoubtedly lead to the development of new and improved monitoring and reporting tools that make new information security data available. It would be advantageous if FISMI could enable organizations to make use of this information in an integrated manner as well. Scalability is an important characteristic of both SIMs (Dubie, 2008) and MISs (Marakas, 2003, p. 440).

3. **Interoperability/compatibility.** Interoperability refers to the ability of different systems made by different manufacturers to work with one another (Pfaffenberger, 1997)**.** As mentioned earlier, organizations commonly use many

different tools (like those mentioned in Chapter 4) to collect information security data. FISMI would have to be able to get the necessary information from these tools. In addition to this, many organizations today have heterogeneous network environments. It is not uncommon, for example, for a company to have some servers that run Microsoft's Windows and others that run Unix operating systems. A framework that allows for interfacing across platforms to gather and report on information security data would, therefore, be of great value. The importance of making SIMs and MISs interoperable and compatible is also recognized (Dubie, 2008; Marakas, 2003, pp. 226, 440).

4. **Distributable**. Organizations may be geographically distributed. It would, therefore, be desirable for FISMI to support such environments.

It has been made clear that information security data will have to be collected from various sources. It would, therefore, also be desirable if the framework provided a way to:

5. **Facilitate new ways of correlating and analyzing data.** To be able to gain a holistic view of the entire information security programme or a specific information security concern, it is necessary to gather information security data from various data sources. It would, for example, be useful to pull together information gathered by different tools with different file formats and application programming interfaces, such as SNORT, Nessus, NetStumbler, Nmap and MBSA. This allows one to find new relationships between the information from each tool, show the history of the specific information gathered and do new forms of analysis on the combined information. Continuous auditing models (Chou, Du, & Lai, 2007), SIMs, the various types of MISs and dashboards typically accomplish this by storing data collected from various sources in data marts or data warehouses.

The objective of this work is the design of a framework that will facilitate the provision of effective management information in the governance of information security to managers throughout the organization. As shown in previous chapters, these managers

differ greatly in both the roles they play in contributing towards information security and their level of technical expertise. Many of the managers that should receive information security reports are not knowledgeable in information security (Nohlberg & Backstrom, 2007, p. 373). It is, therefore, important that the framework allows for the development of tools that are:

6. **Configurable to meet the needs of the different managers**. Chapter 3 has made it clear that different managers will have extremely different responsibilities and amounts of influence when it comes to information security. It has been shown, for example, that a manager in the human resource department, a CIO and the CEO of an organization are all going to have different responsibilities, amounts of influence and interest in information security. It is, therefore, fitting that only the appropriate information security information that pertains to a specific manager is made available to him or her. Popular SIMs, such as Intellitactics SAM, provide the ability to generate different reports and to configure dashboards for different users (Business Wire, 2005). Role-based access and configurable screens are also important characteristics of dashboards (Sardoni, 2002, pp. 15-16).

7. **Able to present information security information in an easy-to-understand manner.** The information should be presented in a manner that shows the state of information security as a whole, or the state of a particular information security concern at a glance (Nohlberg & Backstrom, 2007, pp. 378-379). Managers should be able to see, at an instant, how they are performing their information security duties (Robertson & Raddeman, 2004). This will contribute to enabling managers to take corrective actions as they see that things are going wrong. Interfaces should be easy to operate and require little or no training to use (Marakas, 2003, p. 176). SIMs, MISs, and dashboards commonly achieve this by presenting information in a graphical, tabular and/or textual format (Marakas, 2003, p. 176). Nohlberg and Backstrom also make it clear that an overview of critical information should be given without overwhelming managers with detail. It is, however, valuable if managers are able to access a "wide range of reports including status reporting, exception reporting, trend analysis, drill-down

investigation and *ad hoc* queries" (Marakas, 2003, p. 176). The characteristics listed below can also facilitate the provision of appropriate and meaningful information to different managers.

There are several characteristics that would make it possible for a framework to make information security visible to managers in a way that would be relevant to them. Some of these include that the tool would:

8. **Show Key Performance Indicators (KPIs)**. KPIs can be used effectively to show the overall state of the various information security concerns. The first screen that users see can show KPIs that are of interest to that specific user. Popular SIMs, such as Intellitactics SAM, make use of KPIs to make information security visible in a manner that is meaningful to managers (Business Wire, 2005). When considering the important role that KPIs play in making the appropriate information visible, it becomes evident that organizations should ensure that they are using appropriate indicators (Sardoni, 2002, p. 16). With dashboards, KPIs are often shown using gauges or graphs (Sardoni, 2002, p. 16).

9. **Use metrics**. Like KPIs, metrics are also used commonly to make appropriate information visible in a configurable way in both popular SIM tools and dashboards (Sardoni, 2002). Intellitactics makes very effective use of metrics. This SIM provides a data warehouse that provides access to measures that provide the building blocks of assurance metrics. Dashboards can then be easily generated for multiple users by displaying metrics that show information relevant and appropriate to their roles (Business Wire, 2005).

10. **Have drill-down capabilities.** It has already been emphasized that managers, especially those without much information security and IT knowledge, are more interested in the overall picture of the state of information security or of a specific information security concern. An overview of appropriate information should, therefore, be displayed without overwhelming users with detail. KPIs and metrics can be used to do this. It is also, however, important that users are able to

access the details concerning a certain concern if they so desire (Nohlberg & Backstrom, 2007, p. 379). It is, therefore, necessary that drill-down capabilities are provided. This is an important characteristic of all the classes of tools examined in this chapter. The popular SIM tool, Intellitactics SAM, provides drill-down capabilities. Marakas shows that drill-down capabilities are also an important characteristic of DSSs, showing that such tools commonly provide tools to select, extract, filter and track critical information (Marakas, 2003, p. 176). When discussing executive dashboards, Batchelor also shows the importance of the ability to drill-down for information in providing actionable information. When users are able to not only see the state of an information security concern, but also to drill-down to understand the detail of the problem, they understand why a problem exists and are more likely to be able to take corrective action to address the problem (Batchelor, 2005, p. 29). It is, therefore, fitting that one can drill-down from KPIs to understand the reason for the state of the indicator (Sardoni, 2002, p. 16).

11. **Standards based/measures compliance.** An information security visibility framework will also be of value if it assists managers to measure how well they comply with internationally accepted information security standards. Standards and policies are essential for the proper management of information security (Whitman and Mattord, 2004; Purser, 2004). Security standards, such as ISO/IEC 27002, prove invaluable in helping managers at the governance level to define information security goals, organizational information security standards and effective management practices (ISO, 2006). It is also valuable for information security policy development.

12. **Make use of configurable thresholds.** Chapter 3 highlighted the importance of having agreed-upon security thresholds. This makes it possible that everyone in the organization, from managers at the strategic level to staff at the operational level, has a clear understanding of what the organization finds acceptable and unacceptable with regard to information security. As explained earlier in this

chapter, each organization is unique and, therefore, different organizations have different approaches to information security. A framework for information security visibility should allow for this. It would, therefore, be valuable if the framework allows for configurable security thresholds to be established for the KPIs and metrics used to make the information visible. Ron Hardy, the Chief Strategy Officer for Intellitactics, explains another benefit of making use of configurable thresholds. He reportedly states that, "Security reports and summarized detail lack the context required for executive decision-making. Seeing how a point-in-time measure compares to organizational benchmarks, or being able to identify deviations from normal behavior, increases understanding," Intellitactics SAM, therefore, identifies "areas of high and low performance against targets across the enterprise."

13. **Measure and communicate the progress of security initiatives compared to goals**. This is a characteristic of the tool already mentioned several times in this chapter, Intellitactics SAM. Chapter 3 highlighted the fact that it is an integral part of good ISG to ensure that information security responsibilities and duties are clearly defined and well communicated to all affected staff. This is a key way that managers direct information security. As part of governance, managers should also control the information security programme by ensuring that responsible staff are discharging their assigned duties. It is, therefore, appropriate that a framework that will facilitate the visualization of collated information security management information to all levels of management to support ISG would allow managers to track the progress of specific information security duties or tasks that are assigned to staff. The state of these tasks will often affect the state of the overall information security programme.

In summary, a framework and associated tools for making collated information security management information visible to all levels of management to support ISG would have to be flexible to support various organizations of various sizes and using different, often heterogeneous platforms. It will have to enable the correlation of information security

information from various sources. It should, in addition, make the appropriate and relevant information security information visible to each manager in a configurable, meaningful and easy-to-understand manner.

5.6 CONCLUSION

This chapter has provided a list of characteristics that would be desirable in a framework that will facilitate the visualization of collated information security management information to all levels of management to support ISG. The list has been compiled by studying the finer characteristics of SIMs, management information systems (MISs), decision support systems (DSSs), executive dashboards, compliance dashboards and continuous auditing tools. The characteristics listed in this chapter would be desirable for

any ISG reporting tool, whether it is designed for use in either big or small organizations. These characteristics could be used as a simple checklist for organizations that want to either purchase or develop ISG reporting tools or suites. The characteristics listed in this chapter will, however, be used in this work when designing the framework and choosing from the available tools and technologies that can be used when implementing the framework.

TOOLS AND TECHNIQUES SUITED FOR USE IN THE FISMI

Chapter 6

TOOLS AND TECHNIQUES SUITED FOR USE IN FISMI

6.1 INTRODUCTION

Information technology tools, techniques and design principles that are commonly used today make it possible to create ISG reporting tools that have the desirable characteristics described in Chapter 6. Some of these are briefly discussed in this chapter. The aim of this chapter is not to give a comprehensive understanding of these tools and techniques. The aim is rather to highlight why they are suited to be used in FISMI by showing how they relate to the desirable characteristics for a framework such as the one discussed in Chapter 6.

Service oriented architecture (SOA), data warehousing and portal principles are described. How the use of visualization tools can contribute to the FISMI objectives is also briefly shown.

The section below discusses SOA principles. To understand SOA properly, services and web services are first defined.

6.2 WEB SERVICE – SERVICE ORIENTED ARCHITECTURE

The intention of this section is to make it clear why principles of SOA and the use of web services are suitable for use in the proposed framework that is, amongst other things, flexible, scalable and distributable. To be able to do this, web services and SOA are first defined. The potential benefits associated with making proper use of these are then discussed.

6.2.1 WEB SERVICES DEFINED

Web Service Definitions
A Web Service is: • *"A software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards" (W3C, 2004).* • *"An application stored on one machine that can be accessed on another machine over a network" (Deitel, Deitel, Listfield, Nieto, Yaeger, & Zlatkina, 2002, p. 1041).* • *"An application that exposes a programmatic interface using standard Internet protocols. Web Services are designed to be used by other programs or applications rather than by humans" (Hartman, Flinn, Beznosov, & Kawamoto, 2003, p. 414).*

TABLE 6.1 WEB SERVICE DEFINITIONS

The W3C defines a service as "an abstract resource that represents a capability of performing tasks that form a coherent functionality from the point of view of provider entities and requestors' entities. To be used, a service must be realized by a concrete provider agent" (W3C, 2004). A service is, therefore, something that accomplishes a certain task. An important feature of a service is its autonomy. A service addresses a specific unit of work in an independent manner. One can interface with a service without understanding how that service works. Another important characteristic of web services is that they are very independent of the underlying technology (Sprott, 2005).

There are many different definitions for web services. Some of these are listed in Table 6.1. By studying these definitions, it becomes clear that a web service is, basically, a

service with some special functionality. Erl lists some functionality that is commonly expected from a web service. A web service should generally:

- Communicate via Internet protocols
- Send and receive data formatted as XML documents
- Provide a service description that, at minimum, consists of a WSDL document
- Be able to transport XML documents using SOAP over HTTP
- Be able to act as both the requestor and provider of a service
- Be registered with a discovery agent through which it can be located.

(Erl, 2004, pp. 49 - 50)

Web services are often associated with the use of an SOA. The following section briefly defines it.

6.2.2 SOA DEFINED

Service Oriented Architecture (SOA) Definitions
• *"SOA is an application development methodology that leverages lightweight, well-designed "services" — e.g. customer profile, purchase order, ship to location — registered and maintained in a central repository and available for broad reuse" (Smith, 2008, p. 48).* • *"An SOA is a design model with a deeply rooted concept of encapsulating application logic within services that interact via a common communication protocol" (Erl, 2004, p. 51).* • *"SOA refers to the principles for development and integration of applications; Web services are the set of standards which enable this" (Sebor, 2008).*

TABLE 6.2 SOA DEFINITIONS

As with web services, there are many ways of describing an SOA. Some SOA definitions are listed in Table 6.2.

As can be seen from the above definitions, an SOA is not a tool that can be purchased and customised. The above definitions refer to it as "an application development methodology", "a design model" or principles for application development and integration. This design method promotes the use of services in developing and integrating applications. Web services are often used to implement a service oriented architecture (Erl, 2004, p. 51). Web services and the SOA are, therefore, often discussed together.

Brandt identifies six SOA assumptions. These are summarised below.

1. Applications are loosely coupled. This important concept contributes greatly to the advantages of using SOA principles discussed in the next section. Sprott quotes DeMarco's definition of coupling as "a measure of the interdependence of modules" (Sprott, 2005, p. 11). Modules are highly coupled when changes to one module have a significant effect on other modules. On the other hand, modules are loosely coupled when one module can be modified without having a significant effect on other modules (Sprott, 2005, p. 11). In an SOA, therefore, there are a group of services where a change to one of the services does not significantly impact the other services. The implementations of the services are hidden (Brandt, 2007).
2. Interface transactions are stateless. Interfaces exchange data without storing implicit history.
3. Interfaces follow the RPC (remote procedure call) model. Calling a service interface is similar to calling a local function.
4. The interface is message-based. Messages are sent between applications using an ESB.
5. Messages use XML data. Messages are based on XML data.
6. Interfaces may support both synchronous and asynchronous transactions (Brandt, 2007). When a service is requested, the calling application or service either waits for a response or continues other processing without waiting for the response.

There are entire books devoted to explaining SOA and web services. The brief description of web services and the SOA above is, therefore, not intended to be a comprehensive discussion of the field. SOA principles are used in FISMI. This section, therefore, is included to make the description of the benefits associated with properly implementing the design principles of an SOA clearer.

Some of the general benefits associated with the use of SOA principles are discussed below. How the use of SOA principles can assist in achieving some of the desirable characteristics of FISMI is then made more apparent in section 7.2.4.

6.2.3 General Benefits of using SOA and web services.

The SOA has become a widely accepted architecture among IT users (WinterGreen Research, 2008, pp. 1-1). The many potential advantages associated with applying the SOA design principles have likely contributed to the popularity of SOA.

Effectively implementing SOA principles using web services has some of the following potential benefits:

1. **Enables cross-platform interoperability**. Web services abstract application logic from the underlying technology. They can, therefore, work across diverse, heterogeneous environments on many hardware and software platforms (Hartman, Flinn, Beznosov, & Kawamoto, 2003, pp. 3, 29; Taft, 2008; Deitel, Deitel, Listfield, Nieto, Yaeger, & Zlatkina, 2002, pp. 1041-1042).
2. **Enables distributed computing.** Besides being used within heterogeneous business environments, SOA principles can also be used across physically distributed environments. (Deitel, Deitel, Listfield, Nieto, Yaeger, & Zlatkina, 2002, p. 1040; WinterGreen Research, 2008, pp. 1-1 - 1-3). Applying SOA principles may, for example, make it easier for organizations to take full advantage of grid or cloud computing (Hoque, 2008).
3. **Enables reuse.** Services can be reused.

4. **Makes applications more flexible** (McLaughlin, 2008). Since SOA applications are built around loosely-coupled services, applications can be relatively easily altered as it becomes necessary (Ward-Dutton & Macehiter, 2005).
5. **Can lower costs.** Reuse of services can lower development costs and speed up development (Mccormick, 2007). It is also potentially cheaper to maintain and upgrade SOA-based systems (Garver, 2005).
6. **Allows for quicker response to market changes** (McLaughlin, 2008).
7. **Can be used with legacy applications** (McLaughlin, 2008). Legacy application can be wrapped in services to allow them to integrate with other applications (Erl, 2004, pp. 309 - 310).

6.2.4 BENEFITS OF USING SOA AND WEB SERVICES FOR FISMI

Since the FISMI is based on SOA principles, any implementation based on the framework can potentially realize each of the benefits highlighted above. More importantly though, several of the advantages that are associated with the implementation of SOA principles correspond well to the desirable characteristics for FISMI. The relationship between some FISMI desirable characteristics and the use of SOA principles are shown in Table 6.3 on the previous page.

FISMI desired characteristic	SOA application
Scalability.	With the use of web services, it is relatively easy to either add additional functionality (by adding new services to the SOA system) or enhance existing functionality (by upgrading existing services) so that the information security reporting system can meet the needs of the company at a given time. This is the same principle that gives SOA-based systems the ability to respond quickly to market changes.
Interoperability/compatibility.	SOA application can run on any platform and interact with various applications since web services make business logic available in a platform-independent manner. Web services can also be used to encapsulate/wrap existing applications so that FISMI can interact with them.
Distributable.	SOA principles allow for distributed computing.
Affordable.	By using web services to encapsulate existing information security monitoring applications, FISMI allows organizations to establish a basis for integrated information security reporting with the tools they already have. FISMI doesn't prescribe specific monitoring tools to be used by an organization. Open-source monitoring tools can easily be integrated into FISMI applications. The ability of code reuse with services also lowers development costs.

TABLE 6.3 FISMI CHARACTERISTICS REALISED BY SOA

6.3 DATA WAREHOUSING

Data warehouses have been used successfully for a number of years now. The potential benefits associated with the proper use of data warehouses are well established. Many of the systems mentioned in Chapter 5 are implemented using data warehouses. Continuous auditing systems, MISs, DSSs and SIMs all commonly are created using data warehouses. This subheading summarizes some of the benefits associated with the use of data warehouses that make them appropriate to use for the FISMI. Before the benefits are summarized though, data warehouses are briefly defined.

6.3.1 DATA WAREHOUSES DEFINED

Table 6.4 contains three definitions of a data warehouse. These definitions show that a data warehouse is basically a database that is designed and implemented in a way that enables optimal data retrieval and querying.

Data Warehouse Definitions
A data warehouse is: • *"The conglomeration of an organization's data warehouse staging and presentation areas, where operational data is specifically structured for query and analysis performance and ease-of-use" (Kimball & Ross, 2002, p. 397).* • *"A collection of integrated, subject-oriented databases designed to support the DSS function where each unit of data is relevant to some moment in time. The data warehouse contains atomic data and lightly summarized data. A data warehouse is a subject-oriented, integrated, nonvolatile, time-variant collection of data designed to support DSS needs" (Marakas, 2003a, p. 256).* • *"An inventory of subject-oriented, integrated, and time-variant informational data" (Sperley, 1999, p. 321).*

TABLE 6.4 DATA WAREHOUSE DEFINITIONS

Data warehouses are different from operational databases. Whereas operational databases are usually used to deal with one record at a time, users of data warehouses usually work with many rows that are searched and compressed to produce an answer (Kimball & Ross, 2002, p. 2). The same operational tasks are usually performed repeatedly on operational databases. Conversely, data warehouses are used to answer continuously changing questions (Kimball & Ross, 2002, p. 2). An additional difference is that operational databases are typically normalized to third-normal-form (3NF), whereas data warehouses use dimensional modeling (Kimball & Ross, 2002, p. 11). This work does not describe the process of dimensional modeling and data warehouse design. It is, however, important to note that operational databases use design patterns that reduce redundancy and improve update and insert database transactions. Data warehouses, on the other hand, are designed to optimize understanding, query performance and resilience to change (Kimball & Ross, 2002, pp. 11-12).

The goals of data warehousing have already been touched on in this section. These potential benefits are, however, more clearly listed in the next section.

6.3.2 DATA WAREHOUSE BENEFITS

Data warehouse goals are translated into data warehouse benefits when properly implemented. Some of the potential benefits of using a high-quality data warehouse are described below.

A data warehouse typically contains information from various sources. Having this combined information available in one data warehouse makes it possible to see the complete picture and allows for correlation analysis (Marakas, 2003a, p. 9).

Two of the definitions in Table 7.4 highlight the fact that data warehouses store time-variant informational data. This feature of a data warehouse provides users with the important capability of being able to analyze trends (Marakas, 2003a, p. 9).

Besides enabling historical trend analysis, data warehouses also make information available in a way that users can easily manipulate. To illustrate, with a data warehouse it

becomes easy to drill down into detailed information (Marakas, 2003a, p. 9). Users should be able to slice and dice the information (Kimball & Ross, 2002). This allows users new ways of looking at available information.

One of the primary goals of a data warehouse, as described in the previous section, is to optimize understanding and query performance. Good data warehouses are, therefore, designed so that information is easily accessible, well labelled and intuitive. This makes it easier for all users, including non-IT staff, to access information in the data warehouse (Kimball & Ross, 2002, p. 3; Marakas, 2003a, p. 9).

Data warehouses should also be designed in such a way that they are resilient to change. By following a good data warehouse design methodology, data warehouses should be able to be changed without invalidating existing data or applications (Kimball & Ross, 2002, p. 3).

Another key design principle for data warehousing is to improve query response times. Using a good data warehouse should, therefore, make various types of information available in various formats fast.

The previous section highlighted some general benefits associated with the proper implementation of data warehouses. Table 6.5 shows how using a data warehouse could accomplish some of the characteristics that are desirable for FISMI.

6.3.3 BENEFITS OF USING A DATA WAREHOUSE FOR FISMI

FISMI desired characteristic	Data warehouse application
Facilitate new ways of correlating and analyzing data.	As shown in the previous section, data warehouses are designed to enable new ways of correlating and analyzing data. Instead of information security data being stored in various locations, it is all integrated in a central store.
Able to present information security information in an easy-to-understand manner.	As mentioned, data warehouses are designed for intuitive use. In addition to that, data warehouses also allow users to manipulate data in various ways. They support drill-down capabilities and trend analysis well.
Scalability.	Data warehouses should be designed to be resilient to change.

TABLE 6.5 FISMI CHARACTERISTICS REALISED BY DATA WAREHOUSES

6.4 VISUALIZATION TOOLS

The purpose of this section is not to explain data visualization. It is merely to illustrate its importance.

Data visualization is "the process by which numerical data are converted into meaningful images" (Marakas, 2003a, p. 95). Data visualization can add greatly to a person's ability to understand a complex or large set of data. To illustrate, it is usually easier to spot trends and patterns by looking at graphs than by studying hundreds of rows of numbers.

A framework that makes masses of information security data available to managers with various levels of technical expertise would, therefore, benefit by the use of data visualization.

Table 6.6 summarizes how visualization tools can be used to realize one of desirable characteristics of FISMI.

FISMI desired characteristic	Visualization tool application
Able to present information security information in an easy to understand manner.	It is often easier to make sense of masses of data if it is represented in a visual way.

TABLE 6.6 FISMI CHARACTERISTICS REALISED BY VISUALIZATION TOOLS

6.5 WEB PORTALS

A web portal is "an infrastructure providing secure, customizable, personalizable, integrated access to dynamic content from a variety of sources, in a variety of source formats, wherever it is needed" (Smith M. A., 2004, p. 94). As the name suggests, web portals are usually accessed by web browsers. Portals can be made available either only within an organization, or publicly.

The definition given above highlights several important characteristics and capabilities of portals. Table 6.7 shows how portal capabilities can be used to achieve some of the desirable characteristics for FISMI.

FISMI desired characteristic	**Web portal application**
Scalability.	Portals that make use of web services and portlets are very flexible and have the ability to be adapted easily (Margulius, 2002). By their very nature, web portals are also able to support a range of numbers of users.
Interoperability/ compatibility.	Unlike static web pages, web portal applications can also be used to interact with other application (Smith M. A., 2004, p. 94). A web portal could, for example, be used with several visualization applications to make information more meaningful. As new visualization applications become available, or existing ones improve, they can easily be made to work with the web portal.
Distributable.	Web portals can be used to make information security information available to users even if they are away from the organization. Portals can also be used throughout geographically distributed organizations.
Facilitate new ways of correlating and analyzing data.	As the definition implies, Web portals should have the ability to provide a single point of access to information from multiple sources (Smith M. A., 2004, p. 94). Portals used in conjunction with data warehouses can, therefore, be effectively used to make integrated information available in a manner that allows for new ways of correlating and analyzing data.
Configurable to meet the needs of the different mangers.	Two of the characteristics of portals mentioned in the definition provided are 'customizable' and 'personalizable.' Portals should have the ability to present applicable information in different ways to various users, based on the user's profile (Smith M. A., 2004, p. 94). A FISMI could, therefore, use portal technology to make only the appropriate information security information that pertains to a specific manager available to him or her

TABLE 6.7 FISMI CHARACTERISTICS REALISED BY WEB PORTALS

It should be clear from the above that by applying SOA, data warehousing and portal principles and using good visualization tools, many of the desirable characteristics of FISMI can be achieved.

6.6 CONCLUSION

The technologies and design methods discussed in this chapter are well established. They each have several principles that can enhance general system design where applied properly. In addition to this, they are especially well suited for FISMI since they can be well used to implement some of the desired characteristics for FISMI, as described in Chapter 5. These characteristics include scalability, interoperability and distributability. The design principles can also be used to make information security information visible in a manner that is easy to understand, configurable and facilitates new ways of correlating and analyzing the information.

The next chapter explains how these design methods have been used in FISMI.

FISMI: A FRAMEWORK FOR INFORMATION SECURITY MANAGEMENT INFORMATION

Chapter 7

FISMI: A FRAMEWORK FOR INFORMATION SECURITY MANAGEMENT INFORMATION

7.1 INTRODUCTION

A framework that will make collated information security management information visible to all levels of management to support Information Security Governance (ISG) is described in this chapter. The framework is called FISMI – a Framework for Information Security Management Information. Before FISMI is described, some of the factors that motivate the need for such a framework are discussed. As discussed in previous chapters, some of the characteristics that the framework should incorporate are also summarized below.

7.2 MOTIVATION FOR FISMI

It has already been established that ISG is an integral part of corporate governance and IT governance. Information security should, therefore, be treated as more than merely a technical issue in organizations. Everyone in an organization, from board level down, should be involved somehow with information security. Many of the various information security responsibilities of managers at each level of management have been described in Chapter 3. Some of the key responsibilities that make it clear that a framework such as FISMI and associated tools would be valuable are shown in Table 7.1 below. Table 7.1 makes it clear that at each level of management, managers are responsible for ensuring meaningful reporting regarding the organization's information security status. Strategic managers are required to make sure that the efficiency of information security controls are measured, tracked and monitored so that proper reporting can take place. Taking into account the complex and changing nature of security controls, it becomes necessary for this tracking and monitoring to take place in an automated fashion.

Managers' ISG responsibilities with regard to information security reporting
Managers at strategic level: 8. Develop and introduce clear and regular reporting on the organization's information security status to the board of directors based on the established policies, guidelines and applicable standards. Report on compliance with these policies, important weaknesses and remedial actions, and important security projects. 9. Track the closure of recommendations made after information security audits based on clear process and accountabilities. 10. Insist that management make security investments and security improvement measureable, and monitor and report on programme effectiveness.
Managers at tactical level: 11. Provide strategic managers, like the board and CEO, and organizational unit heads with the relevant meaningful information security information that will help these managers to discharge their information security responsibilities. 12. Be aware of and understand their personal information security responsibilities as assigned to them by the organization.
Managers at operational level: 13. Be aware of and understand their personal information security responsibilities. 14. Comply with all the information security responsibilities put upon them by the organization. 15. Report any information security vulnerabilities or incidents in the appropriate way.

TABLE 7.1 MANAGERS' ISG RESPONSIBILITIES WITH REGARD TO INFORMATION SECURITY REPORTING

Chapter 4 made it clear that, although significant progress has been made in the field of information security reporting tools, there is still a need for an affordable way of making information security information visible to all managers in smaller organizations that do not have the resources required by the commercial SIMs like Intellitactics that provide

this facility. A framework that will make collated information security management information visible to all levels of management to support ISG will, therefore, assist various managers in discharging their information security responsibilities. Such a framework can serve as a guide when developing tools that provide managers at different levels with meaningful, relevant information security information. FISMI attempts to achieve this.

To be able to do this effectively, FISMI will have to be designed to incorporate the desirable characteristics for an ISG reporting tool as listed in Chapter 6. These characteristics are shown in Table 7.2. Based on this work, the following section describes FISMI.

Desirable characteristics of an ISG reporting tool
1. *Scalable.*
2. *Interoperable/compatible.*
3. *Distributable.*
4. *Affordable.*
5. *Able to facilitate new ways of correlating and analyzing data.*
6. *Configurable to meet the needs of the different managers.*
7. *Able to present information security information in an easy-to-understand manner.*
8. *Use Key Performance Indicators (KPIs).*
9. *Use metrics.*
10. *Have drill-down capabilities.*
11. *Be standards based/measures compliant.*
12. *Make use of configurable thresholds.*
13. *Measure and communicate the progress of security initiatives compared to goals.*

TABLE 7.2 DESIRABLE CHARACTERISTICS OF AN ISG REPORTING TOOL

7.3 FISMI

As noted before, the acronym FISMI stands for Framework for Information Security Management Information. This section provides the context for the description of FISMI by briefly describing what a framework is.

A framework has been simply defined as "the main part on which the rest is built" (Deam, Rathbone, Waite, & Manser, 1984). A framework, like an architecture, is something that indicates the structure of a system (Fowler & Fowler, 1969, p. 325; Rozanski & Woods, 2005, p. 12). As such, it is used to highlight the essential aspects of a system (Olivier, 1997, p. 53). Some of the essential aspects of the system include:

- the components of the system;
- the relationships between these components;
- and the principles that govern the 'evolution and design' of the system (Macaulay, 2004, p. 4).

Frameworks are used as blueprints when designing new systems. FISMI is, therefore, designed so that it can be used as a guide for organizations that wish to implement systems that will support managers with regard to ISG.

The desirable characteristics for tools that support ISG (Table 7.2) are the principles that govern the design of FISMI. The next section describes the components of FISMI and the relationships between them.

7.3.1 FISMI DESCRIBED

FISMI promotes a toolset approach to ISG reporting. Essentially, the framework consists of a number of web services that collect information security related information from various sources and store the information in a data warehouse. This information can then be made visible to managers using various visualization tools. In order to make the information meaningful to users, the information is linked to KPIs, metrics, company goals, information security standards and information security responsibilities. Figure 8.1 illustrates these essential components.

FISMI uses a similar approach to that employed for information gathering by SIM tools. Information security data is collected, normalized, aggregated, correlated and archived from various data stores. The combined information is then visualized (Mitropoulos, Patsos, & Doulgigeris, 2007, pp. 228-230; Shipley, 2006). To be able to do this in a manner that can be used in potentially very heterogeneous and distributed environments, the framework makes extensive use of web services and adheres to the principles of a Service Oriented Architecture (SOA). The various components of FISMI are described in more detail below.

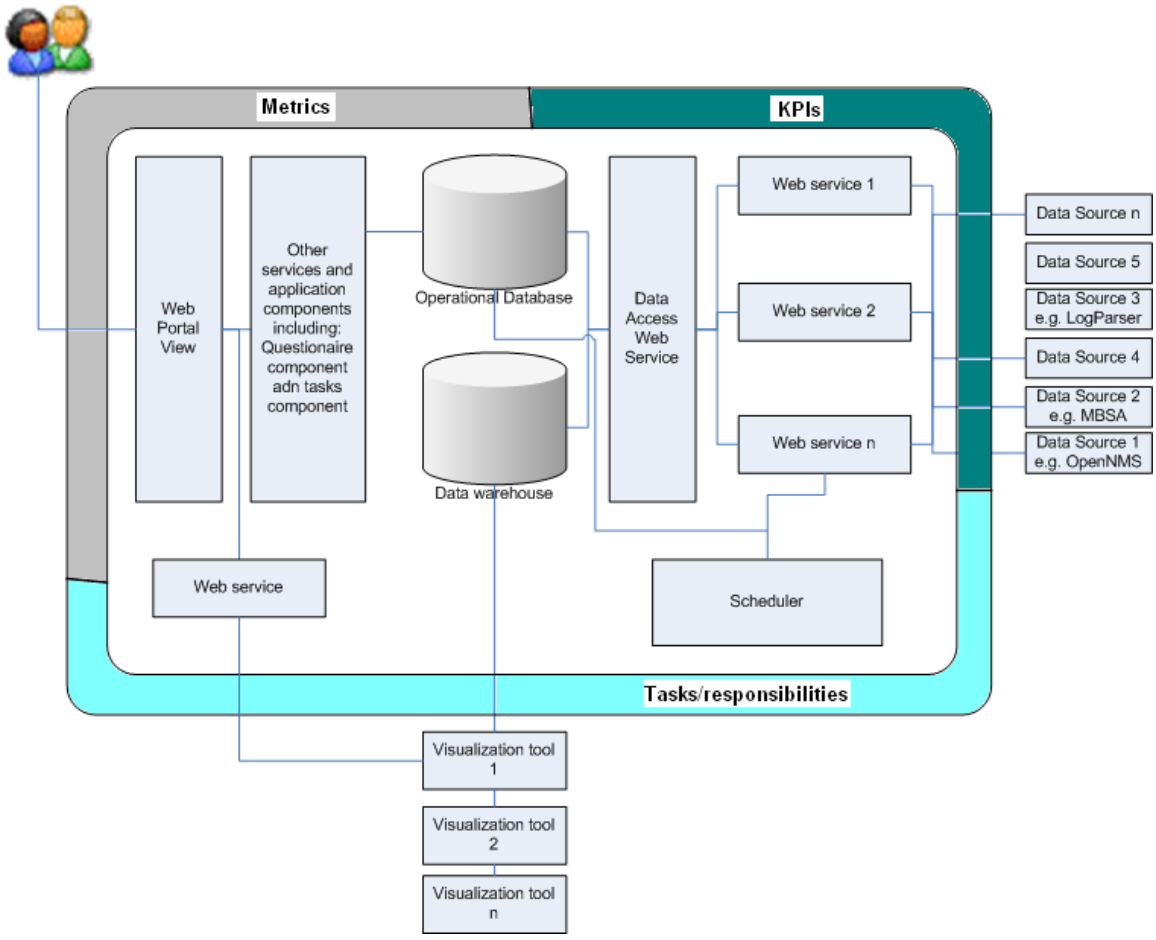


FIGURE 7.1 FRAMEWORK FOR INFORMATION SECURITY MANAGEMENT INFORMATION

Various organizations may have a variety of tools, systems and processes they employ to gather information security related data. For the purposes of this discussion, these will be referred to as **information security data sources**. Vastly different tools may be used by

different organizations depending on their needs, budget and preferences. These tools may include single-purpose information security tools (such as anti-virus tools, firewalls or vulnerability scanners) and/or Security Information Management (SIM) tools as described in Chapter 4. There is no single tool, to the knowledge of the researcher, which can accomplish every information security function as efficiently as a group of separate tools can. To illustrate, there is no single tool that can accomplish anti-virus protection and virus reporting, intrusion detection and access control as well as the best of each tool in each category can achieve separately. FISMI, therefore, promotes a toolset approach where various 'best-of-breed' solutions can be used to capture and analyze information security data. Organizations that are limited with regard to the information security tools that they use to gather data because of various factors such as resources, skills and company size may still be able to utilize FISMI to support ISG.

Other sources of information security data in organizations could include internal and external audit reports and questionnaires. Depending on the organization, the content, volume and format of this information could be very different.

FISMI allows organizations to use whatever information security data sources they may require by using **web services** to encapsulate the various data sources. These web services are run periodically by a service referred to as the scheduler. The scheduler invokes the web services that encapsulate the data sources based on information stored in a database. When invoked, these web services interface directly with the data access web service which then stores the data in the appropriate place in the data warehouse. Web services and the benefits that are associated with implementing them properly have been described in Chapter 6. The benefits associated with the use of web service in FISMI are again listed and applied in the paragraphs below.

One of the main benefits of using web services for FISMI has been described above. The use of loosely-coupled services makes applications more flexible and allows for quicker response to market changes (McLaughlin, 2008). Chapter 6 made it clear that applying SOA principles makes integration of applications possible by encapsulating application logic in web services that communicate by means of a common communication protocol. With FISMI, the necessary information security data is, therefore, retrieved and

communicated by encapsulating various data sources within web services. This can be applied to even legacy information security systems.

Using web services also enable cross-platform interoperability (Hartman, Flinn, Beznosov, & Kawamoto, 2003, pp. 3, 29; Taft, 2008; Deitel, Deitel, Listfield, Nieto, Yaeger, & Zlatkina, 2002, pp. 1041-1042). As mentioned in Chapter 6, web services abstract application logic from the underlying technology. They can, therefore, work across diverse, heterogeneous environments on many hardware and software platforms. This is a valuable feature for FISMI since different information security tools that are encapsulated as information security data sources, visualization tools and databases may be run on different hardware or software platforms even within a single organization.

In addition, web services enable distributed computing. SOA principles can also be used across physically distributed environments. (Deitel, Deitel, Listfield, Nieto, Yaeger, & Zlatkina, 2002, p. 1040; WinterGreen Research, 2008, pp. 1-1 - 1-3). FISMI could, therefore, be applied by not only very small to larger local companies but even by large organizations that operate internationally.

Chapter 6 identified affordability as an important desirable characteristic for FISMI. FISMI should be able to be implemented in an affordable manner if SOA principles are properly applied when organizations use FISMI as a blueprint for ISG automated systems. FISMI makes it possible for organizations to develop an automated ISG system by using information security tools, visualization tools, databases and other system components that organizations either are already using, that are open source or that the organization can afford. SOA principles also promote code reuse. A service that is used to retrieve and communicate information security data may, for example, be used to encapsulate more than one data source. Following SOA principles also potentially make systems based on FISMI cheaper and easier to maintain and upgrade.

Once the information security data is in the **data warehouse,** various applications or agents can be used to normalize, aggregate, correlate and analyze the information. Different **visualization tools** can also be used to manipulate and visualize the data. Chapter 6 showed that other benefits associated with using a data warehouse to store

information security data. They include the fact that data warehouses should be designed so that they are resilient to change. They are also designed for intuitive use. They can, therefore, be effectively used to present information security information in an easy-to-understand manner.

Another component of FISMI is the **web portal**. Different people have access to diverse information and view it differently based on their role-based access to the web portal.

Having a central store for information security data alone does not provide managers with a meaningful ISG solution. The information must be presented in a meaningful, actionable way to be able to facilitate ISG. As mentioned in previous chapters, it is also essential that this framework allows for each manager involved with ISG to be presented with applicable, meaningful information. This can be challenging since what is important information security information to one manager may be of absolutely no value to another. FISMI makes use of several techniques used to organize and structure the collated information security data so as to ensure that the appropriate information is presented to various managers in a meaningful way. These are highlighted in the following section.

It is firstly, however, important to note that one of the key principles that FISMI adheres to is that organizations should benefit from following guidelines set out in information security standards and best-practice guidelines such as ISO/IEC 27002 and CoBIT. As is seen in the following discussion, this principle influences many of the design decisions made in FISMI.

To achieve a holistic view of the performance of an information security program, FISMI encourages organizations to identify main security areas. These main security areas give an overall view of the organization's information security landscape. FISMI adheres to a standards-based approach to information security. So, although organizations may choose main security areas that suit their specific organization, FISMI recommends aligning main security areas with those identified in recognized information security standards. To illustrate, some of the main security areas identified by ISO/IEC 27002 include security policy, human resource security and physical and environmental security (Thiagarajan,

2006). The performance of the controls associated with these security areas should be measured and reported on. The main security areas are hereafter referred to as key performance indicators (KPIs).

A KPI will have various metrics associated with it. These metrics measure the effectiveness of controls that are linked to the KPI. Organizations should also be guided by best-practice information security standards when choosing controls. The information needed for the metrics will be stored in the data warehouses and may come from any of the various sources mentioned in the previous section including information security tools (for example, anti-virus tools), questionnaires (for example, organizations may complete a questionnaire such as the SAN's audit checklist (Thiagarajan, 2006)) and internal and external audit results. Like various successful management tools, FISMI allows various users to register to see various KPIs and metrics.

FISMI includes an automated, standards-based information security **questionnaire component**. This component is not merely a data source: it allows managers to configure desired performance levels for KPIs and metrics. Managers are encouraged to set values for the minimum level of performance that will be accepted and the desired level of performance. The actual level of performance will either be measured using available data or will be set by the relevant manager where it cannot be determined in another manner. Managers are also encouraged to weight various metrics to indicate how importantly the organization views them. The ability of appointed managers to be able to set the values for what the organization is willing to accept and what they actually desire for each KPI makes the organizations security objectives/goals clear; thus, providing direction. Making actual performance levels visible in relation to acceptable and desired performance levels also assists managers to see where corrective action is necessary. Making performance levels visible in this manner, therefore, assists managers to *direct* and *control* information security in harmony with best-practice information security standards.

When making information available to various managers in a way that will assist them in ISG, it is important that the information is linked to the individual's ISG responsibilities. FISMI, therefore, has a **tasks component**. It is possible to assign tasks to various staff.

The tasks progress is then monitored. The task progress is updated by users to reflect whether the tasks progress is *acceptable*, *good* or *unacceptable*. A task is also assigned as critical or not. Tasks can be linked to KPIs. A critical task's progress can, therefore, affect the state of a KPI. Each individual will be presented with the information about the progress of his/her task when he/she logs on to the portal. Managers of departments can also track the progress of information security tasks within their department.

FISMI can be configured so that a user or user group is shown either the 'health' of specific KPIs (or key security areas), specific metrics, progress of tasks or a combination of these that are applicable to the user. To illustrate, a member of the board could log on to the system and be presented with a dashboard that indicates whether the organization's standards-based information security goals are being achieved or not. The dashboard would indicate this by showing the level of performance for each KPI in comparison to the organization's desired level of performance and the level of performance that is deemed acceptable. The board member may see a security area that may need attention. He or she could then drill down and see the metrics that are associated with this area. The director of the human resource (HR) department of the same company would, however, see very different information when logging on to the system. The HR director may, for example, be presented with information that shows the performance of the HR security KPI. He or she may also see the progress of information security tasks that have been assigned to him or her or to other members of the department.

As can be seen above, FISMI provides a means of effectively gathering information security data from various sources throughout any organization. It also provides managers with a standards-based and actionable way of looking at information security information.

The following section highlights some of the benefits associated with FISMI.

7.3.2 FISMI BENEFITS

Making use of FISMI effectively has several advantages associated with it. This section firstly highlights the benefits of FISMI that were also described as desirable

characteristics for such a framework previously. The subheading following discusses additional benefits associated with FISMI.

7.3.3.1 FISMI DESIRABLE CHARACTERISTICS

The previous section has already mentioned how FISMI implements many of the desirable characteristics listed in Table 7.2. Many of the points mentioned below, therefore, serve as a summary for what has been mentioned previously.

1. *Scalable.* As highlighted in this chapter, FISMI allows for a system that would accomplish this by making use of a service-oriented architecture approach. The use of web services to encapsulate existing tools makes sense for a number of reasons. Different organizations may, for many reasons, have a wide array of monitoring tools that collect information security information running in their organizations. With this architecture, when a new tool becomes available, it is easy to retrieve the information it exposes by writing a new web service that can interface with the tool or make use of an existing web service. Which web service should be called, how often this should be done and other information to do with the invocation of this service must then simply be added to the operational database from where the scheduler will retrieve it and invoke the service. The service will, in turn, have the responsibility of interfacing with the data access web service to store the data in the appropriate place in the data warehouse. As can be seen, this approach to gather information is very extensible because new tools and the metric associated with these tools can easily be integrated into the system as the need arises.
2. *Interoperable/compatible*. Web services are commonly used to provide a standard way of remotely invoking functionality across different platforms (Kalani and Kalani, 2003, p 288-290).
3. *Distributable*. Web services are commonly used to provide a standard way of remotely invoking functionality across different platforms (Kalani and Kalani, 2003, p 288-290).

4. *Affordable*. As mentioned previously, FISMI makes it possible for organizations to develop an automated ISG system by using information security tools, visualization tools, databases and other system components that organizations either are already using, that are open source or that the organization can afford. SOA principles also promote code reuse. A service that is used to retrieve and communicate information security data may, for example, be used to encapsulate more than one data source. Following SOA principles also potentially make systems based on FISMI cheaper and easier to maintain and upgrade.
5. *Able to facilitate new ways of correlating and analyzing data*. A characteristic of an FISMI is that it will facilitate new ways of correlating and analyzing data. To meet this objective, the FISMI architecture makes use of a data warehouse to store the information security data gathered. Within the data warehouse there is a general-purpose star schema that can be used to store the general information about metrics. If this general purpose schema does not meet the needs of the metric and information that has to be stored in relation to it, another star schema will have to be added to the warehouse. Data warehouses are designed especially so that this type of analysis can be done efficiently and easily to improve decision support (Kimball & Ross, 2002).
6. *Configurable to meet the needs of the different managers.* The previous section illustrated how FISMI can be configured to suit the needs of different user groups by associating users with appropriate KPIs, metrics and tasks.
7. *Able to present information security information in an easy-to-understand manner*. See characteristics 8 – 12. In addition to using the characteristics listed below, FISMI also allows for various visualization tools to be used.
8. *Use Key Performance Indicators (KPIs)*. FISMI uses KPIs. It is recommended that KPIs are based on best practice guidelines.
9. *Use metrics*. FISMI uses metrics. Metrics may be linked to KPIs. Different metrics may be presented to various managers.
10. *Have drill-down capabilities*. FISMI supports drill-down capabilities. This will be more clearly illustrated with the prototype in the next chapter.

11. *Be standards based/measures compliant*. FISMI promotes a standards-based approach in determining KPIs and thus, information security goals. It also promotes adherence to guidance provided by best-practices information security standards when determining controls. It also includes an automated, standards-based information security questionnaire component.
12. *Make use of configurable thresholds*. With FISMI, users can use the automated, standards-based information security questionnaire component to set values that indicate what level of performance they view as acceptable and desirable for any given KPI and control.
13. *Measure and communicate the progress of security initiatives compared to goals*. FISMI accomplishes this by showing actual performance of security initiatives in relation to set desired levels of performance.

7.3.3.2 WHY FISMI SUPPORTS ISG?

In the introduction to this dissertation the primary objective of the work was described as the development of a framework that will facilitate the provision of effective management information in the governance of information security for organizations with limited resources. This section shows how FISMI achieves this. It firstly summarizes some of the points listed above to show how FISMI can be used in organizations with limited resources and then how it can be used to provide effective management information. It finally highlights why it can be said that FISMI can be used to support ISG.

It has been demonstrated that FISMI can be effectively used by organizations with limited resources. FISMI does not compel organizations to make use of expensive information security tools. The framework makes it possible for organizations to develop an automated ISG system by using information security tools, visualization tools, databases and other system components that organizations are either already using, that are open source or that the organization can afford. SOA principles, also, promote code reuse. A service that is used to retrieve and communicate information security data may, for example, be used to encapsulate more than one data source. Following SOA

principles also potentially make systems based on FISMI cheaper and easier to maintain and upgrade. The prototype system demonstrates how FISMI can be applied affordably. The next chapter describes a prototype system based on FISMI. It will show that in implementing the prototype system (ISMIPS) the researchers made use of tools that were already at their disposal. No information security tools were purchased. ISMIPS also uses a free open source information security tool and database software to illustrate what can be achieved using existing free systems.

It has also been demonstrated that FISMI can be used to provide effective management information. Some of the ways in which this is achieved is by designing FISMI in such a way that it can be used to develop systems that are configurable to meet the needs of the different managers and able to present information security information in an easy to understand manner. It accomplishes this by using Key Performance Indicators (KPIs), metrics and configurable thresholds so that progress of security initiatives can be measured and communicated compared to goals. FISMI also allows users to drill-down for additional information by linking security areas, metrics and tasks. Importantly, FISMI promotes a standards based approach in determining KPIs and thus information security goals. It also promotes adherence to guidance provided by best practices information security standards when determining controls. It also includes an automated standards based information security questionnaire component. Linking security initiatives to standards based business goals, security controls and information security tasks or responsibilities allows for presenting information security information in a manner that is meaningful to managers.

FISMI can additionally be used to assist in ensuring ISG. It is important to note that FISMI will not cause or ensure ISG, rather that it can be used to assist managers in implementing ISG. Governance is primarily about leadership (Institute of Directors, 2002) and as such can only be achieved by managers; not by frameworks or systems. A framework can, however, be used to assist these managers to realize ISG and this section describes how FISMI can be used to do so.

Part of the reason that FISMI can be used to support ISG activities is that FISMI promotes a best practice approach to information security and is not merely a system

architecture for a software tool that allows for information security reporting. If FISMI is to be used optimally in an organizations managers will be forced to consider factors such as which information security standard they are going to adopt, what level of performance the organization is willing to accept and what the organization's goals are for each security control and which metrics they are going to put in place to measure security controls. Managers are also encouraged to assign information security tasks that can be monitored to employees. Besides providing an organization with appropriate automated information security reports about collated information security data, FISMI can, therefore, be used in conjunction with other ISG activities. The following section makes this clear by explaining how FISMI can be used within the *direct-control cycle* mentioned in chapter 2.

The Von Solms and Von Solms (2006) direct-control cycle for ISG was presented in Chapter 2. The cycle basically describes how directives for ISG developed at the strategic level of management are filtered down through the other levels of management. This is the direct part of the direct-control cycle. Von Solms and Von Solms also highlight how the ISG process is controlled by bottom-up compliance reporting. At the operational level, information security information is collected. At the tactical level, this information is compiled and integrated to produce reports that highlight the status of information security to the strategic level in an aggregated format. Figure 7.2 illustrates how FISMI could be used in the ISG direct-control cycle.

As Figure 7.2 illustrates, there are various means that managers use to direct information security. FISMI could assist managers to direct information security in various ways. As mentioned previously, in the process of implementing FISMI managers are required to decide on information security goals. FISMI can also be used to assign information security tasks to employees. FISMI can then be used to make the directives and information security goals more visible to employees. By measuring and monitoring the progress of security and reporting the results in a meaningful manner to various managers FISMI also provides information that managers need to see, where corrective action is necessary and control information security initiatives. By scheduling that information

security tools (like anti-virus tools) are run periodically FISMI can also play a role in executing information security directives.

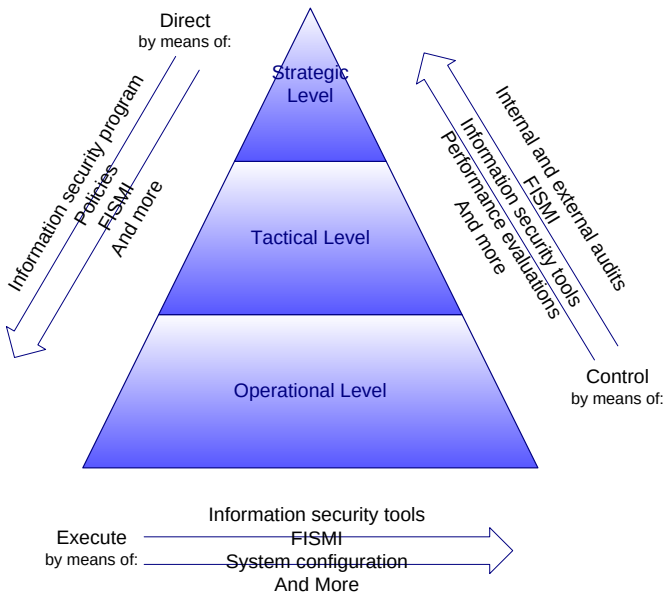


FIGURE 7.2 FISMI IN RELATION TO THE DIRECT-CONTROL CYCLE

In chapter 2 Von Solms was quoted as defining ISG as follows: "Information Security Governance is an integral part of corporate governance, and consists of the management and leadership commitment of the board and top management towards good information security; the proper organizational structures for enforcing good information security; full user awareness and commitment towards good information security; and the necessary policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people, etc) are maintained at all times" (Von Solms, 2006, p. 167). From this definition it is clear that user awareness and commitment towards information security is an important component of ISG. FISMI can be used to improve user awareness and commitment to information security by presenting the appropriate information security information to everyone. This

includes presenting managers with information regarding specific information security tasks or responsibilities assigned to them or their department.

In addition to this, FISMI can assist managers to fulfill their ISG responsibilities. There are two general responsibilities that every manager has to ensure proper ISG. These can be seen in Table 7.1. All managers must ensure that information security is properly reported. This has to be done in an automated fashion, and FISMI provides an easy and affordable way of doing this. All managers must also make sure that they are aware of and comply with their information security responsibilities. Using FISMI effectively, managers may assign information security tasks that are linked to security areas or controls to employees. The progress of these tasks can then be tracked and is made visible to the responsible employee. FISMI, therefore, can be used to assist all managers to perform their core ISG responsibilities.

7.4 CONCLUSION

FISMI has several features that make it a desirable approach to follow when implementing tools to improve visibility of information security in an organization and to use as a means to aid in better management of information security throughout an organization.

By following a standards-based approach and making use of technologies such as web services, data warehouses, operational databases and visualization tools, the framework should also be able to be used to enhance the visibility of information security in the organization. It should also allow for a customizable, summarized and comprehensive overview of information security concerns to managers. This should, in turn, help managers to direct and control information security concerns more efficiently. The principles of service-oriented architecture applied in the design of the architecture also make the FISMI scalable, interoperable, affordable and distributable.

The next chapter further highlights the practical value of FISMI by describing a proof-of-concept prototype.

INFORMATION SECURITY MANAGEMENT INFORMATION PROTOTYPE

Chapter 8

INFORMATION SECURITY MANAGEMENT INFORMATION PROTOTYPE

8.1 INTRODUCTION

This chapter briefly describes a prototype system that has been implemented based on FISMI. The prototype system is called ISMIPS – Information Security Management Information Prototype System. ISMIPS serves as a proof-of-concept system that attempts to prove that all concepts defined in FISMI can actually be implemented successfully. This chapter firstly describes how ISMIPS has been implemented, founded on the principles outlined in FISMI. Examples of how ISMIPS can be used are then given to more clearly demonstrate some of its features.

8.2 ISMIPS IMPLEMENTATION DESCRIPTION

The main components of FISMI have been described in the previous chapter. These components include the:

- information security data sources,
- data warehouse,
- visualization tools,
- web portal,
- various web services,
- standards-based information security questionnaire component,
- and tasks component.

The relationships between these components are summarized in Figure 7.1 in the previous chapter. This section describes how each of these components has been implemented in ISMIPS.

To demonstrate that it is possible to collect information security data from different information security tools, ISMIPS used Microsoft Baseline Security Analyzer (MBSA) and OpenNMS as **information security data sources**. Each of these tools is discussed in Chapter 4. As recommended in FISMI, ISMIPS uses **web services** to interface with these tools. The web service which interfaces with MBSA, the *MBSAparser service*, collects information gathered by the MBSA software about updates on the network. Similarly, the web service that interfaces with OpenNMS, the *OpenNMSparser service*, retrieves information that is gathered by OpenNMS about service availability. The *OpenNMSparser* and *MBSAparser* web services interface with another web service called the *DBAccess service* that is responsible for interfacing with the data warehouse and the operational database. The *DBAccess service* inserts the appropriate update and service availability data into the appropriate star schemas in the data warehouse.

Both the operational database component and the **data warehouse** components of ISMIPS have been implemented as postgres databases in the initial prototype. The operational database includes tables that store information about users, the roles these users will be assigned to, scheduled jobs (including information like how frequently the job must run, arguments that must be passed to the job, etc.) and about metrics (including display information such as descriptions for the metrics and values like the weighting, desired value, actual value and minimum acceptable for the metrics). The operational database also stores the relationships between roles and metrics and roles and security areas.

The data warehouse has specific star schemas to store information about update and service availability metrics and a general-purpose star schema that can be used when extending the prototype to include different metrics. This star schema includes a *health-level_fact* table and *date* and *fact_type* dimension tables.

The scheduler service is the software component that uses the information in the operational database to invoke the execution of the web services that interface with the information security data sources like OpenNMS and MBSA.

Before describing the implementation of other ISMIPS components, it is worth noting the ability of ISMIPS to run in a heterogeneous environment. ISMIPS collects update and service availability information from two tools that run on Microsoft operating systems. The web service and web interface were also created using Microsoft's Visual Studio.Net. All these components, however, interface and communicate easily with the postgres data stores on a Linux platform.

ISMIPS also implements a standards-based information security **questionnaire component**. The questionnaire is based on the SANS audit check list, referred to in section 7.3.1 of the previous chapter. It was implemented as part of an ASP.net application. The automated questionnaire is presented as a web form where users are required to set a minimum acceptable level of performance, the desired level of performance, actual level of performance and a weighting to show importance for each control identified in the questionnaire. Figure 8.1 is a screenshot of this.

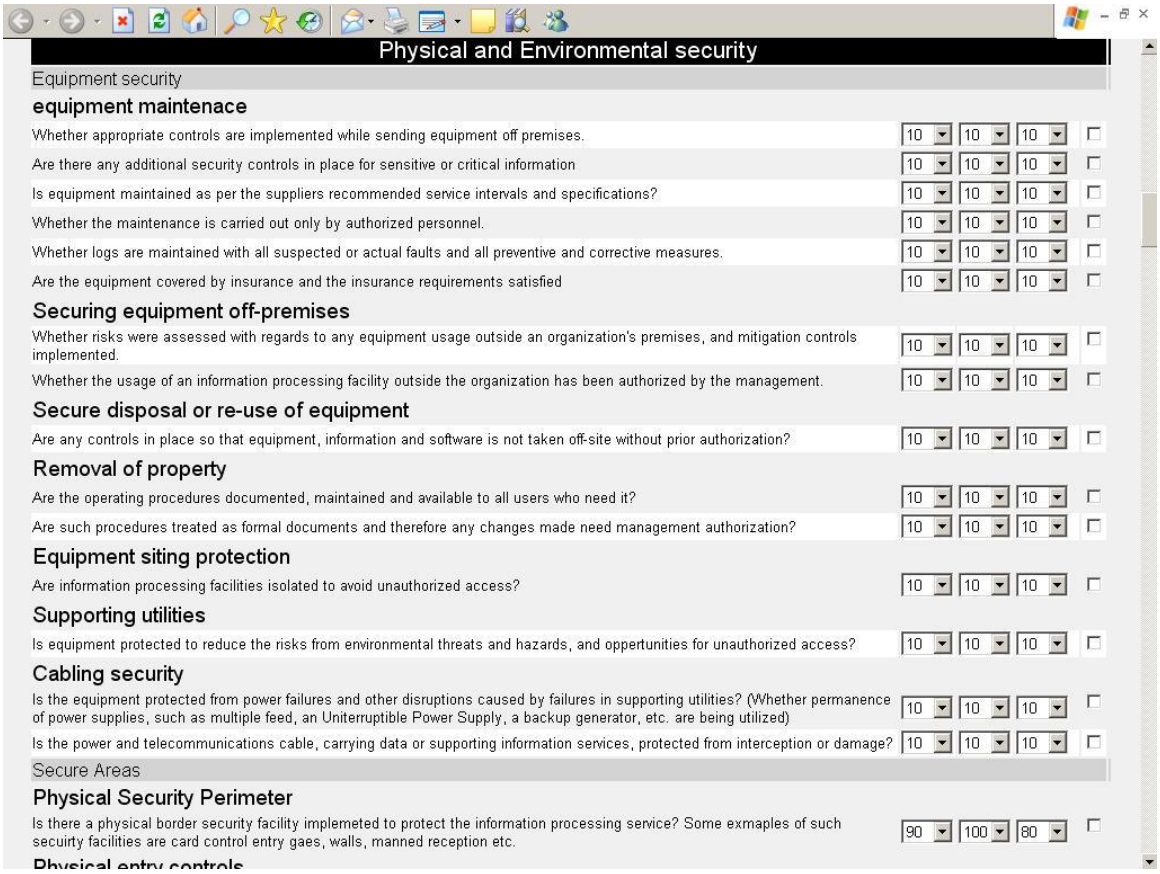


FIGURE 8.1 ISMIPS QUESTIONNAIRE COMPONENT SCREEN

A **tasks component** is also included in the ISMIPS web application. Here, users are allowed to assign information security-related tasks to staff. The interface also allows users to update the progress of each task.

The initial prototype system has a **web interface** created in ASP.net. As mentioned previously, the operational database maps specific users to roles and roles to metrics and security areas or KPIs. Roles will also have links and news associated with them. With these mappings, each user that logs on to the system will be able to see only the information that applies to him or her.

The following section will give two examples of how users may use ISMIPS.

8.3 ISMIPS USAGE EXAMPLE

This section highlights some of the features of ISMIPS by showing and explaining two examples of how the system may be used. The first example shows how a CIO may view information collected by ISMIPS. The second example demonstrates how ISMIPS could be extended to include new information security tools and metrics.

8.3.1 VIEWING ISMIPS INFORMATION

This section briefly shows how a manager, using ISMIPS, may be presented with information security information. Screens that a CIO might see as well as a screen that an HR manager may see are shown.

Figure 8.2 shows a screenshot from ISMIPS that a CIO of a company may be presented with. The CIO is likely to want to see at a glance the health of all security areas in his/her organization. ISMIPS may, therefore, be used to show the CIO the level of performance for each of the security areas that are identified as deserving of attention by a well-recognized information security standard (ISO/IEC 17799:2005). Figures 8.3 and 8.4 show how actual, acceptable and desired performance levels for each security area are indicated. By showing the CIO how the actual level of performance for each security area

compares with what the organization has identified as an acceptable level of performance, allows the CIO to easily see which security areas need attention. The CIO is also able to see how the actual performance compares to the organization's security goals or desired level of performance for each security area.

The CIO would also have the ability to drill down for more information. He or she may, for example, be concerned that information security compliance in the organization is not acceptable. By clicking on the "more" link under the compliance security area, the CIO would see the screen depicted in Figure 8.4. This screen shows the questionnaire results, metrics and tasks that affect the performance of the compliance security. Figures 8.5 and 8.6 indicate how the CIO could drill down for even more information.

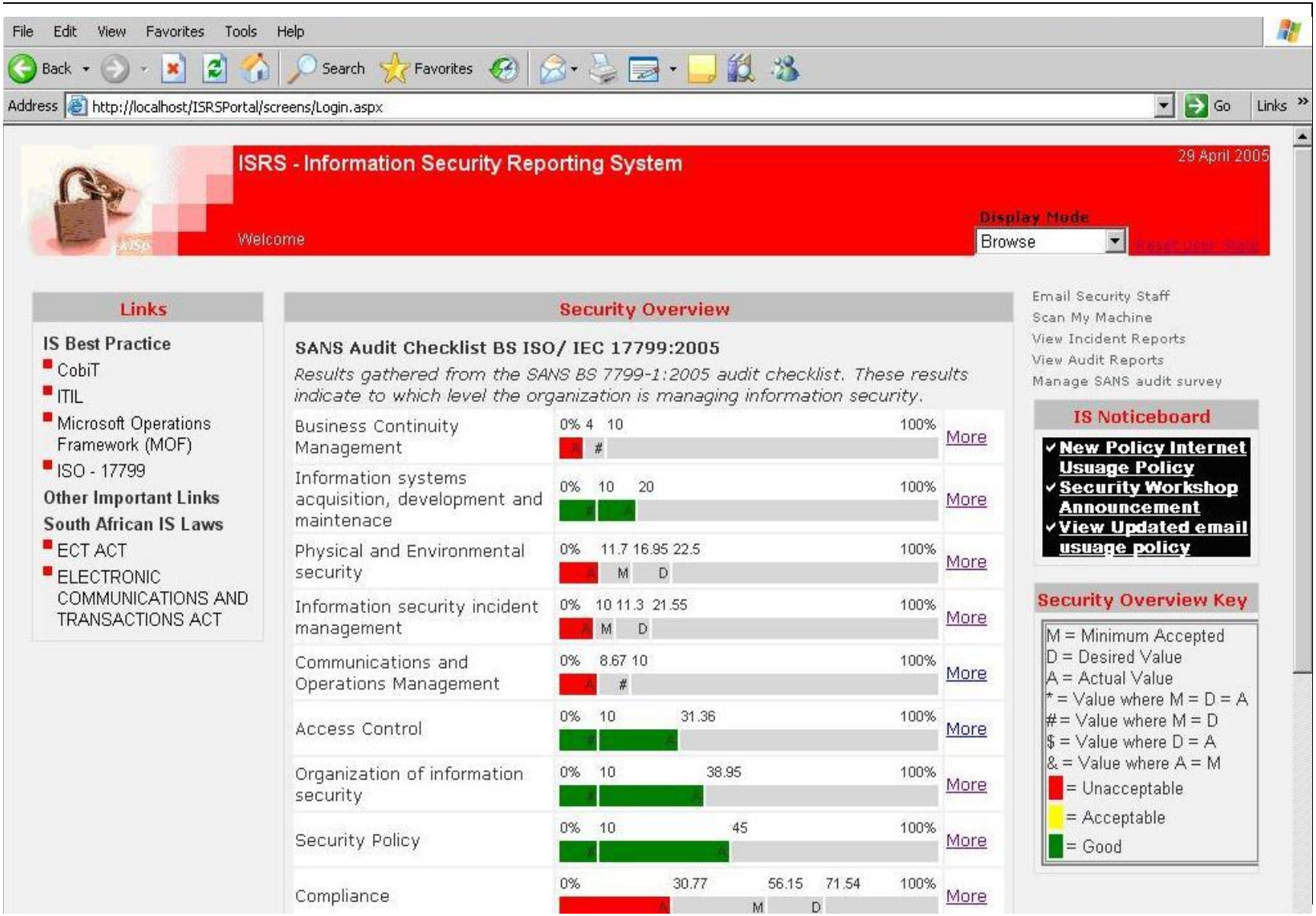


FIGURE 8.2 SAMPLE ISMIPS SCREEN

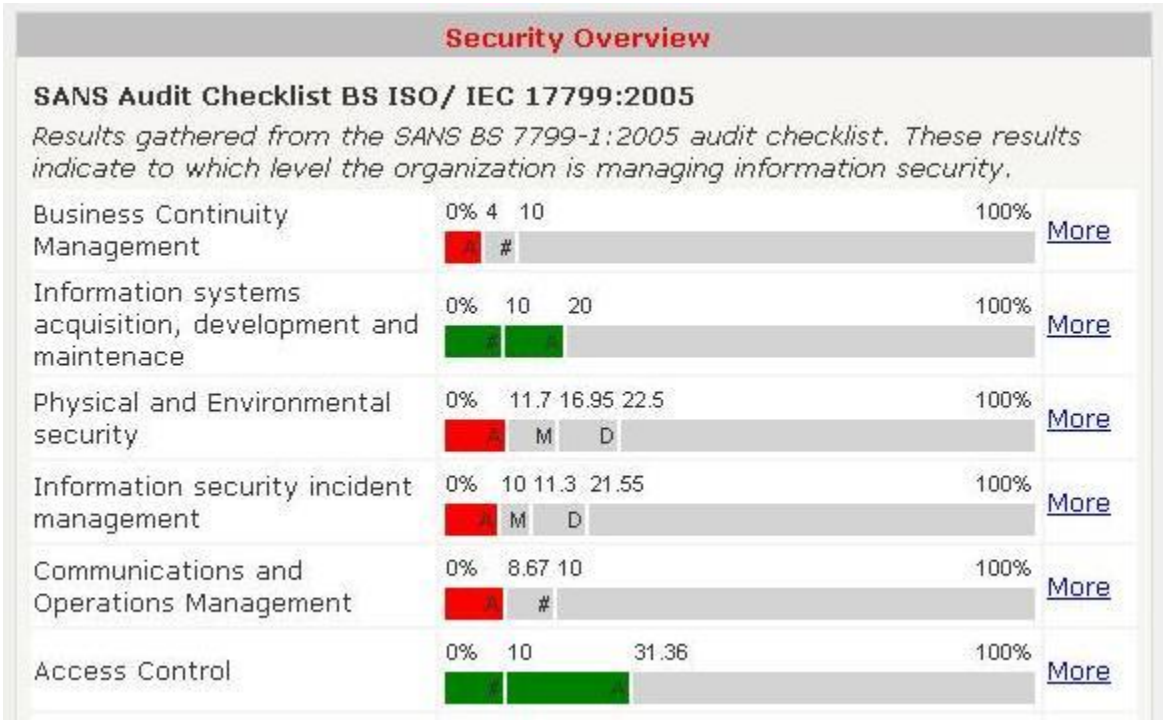


FIGURE 8.3 ISMIPS SECURITY OVERVIEW REPRESENTATION

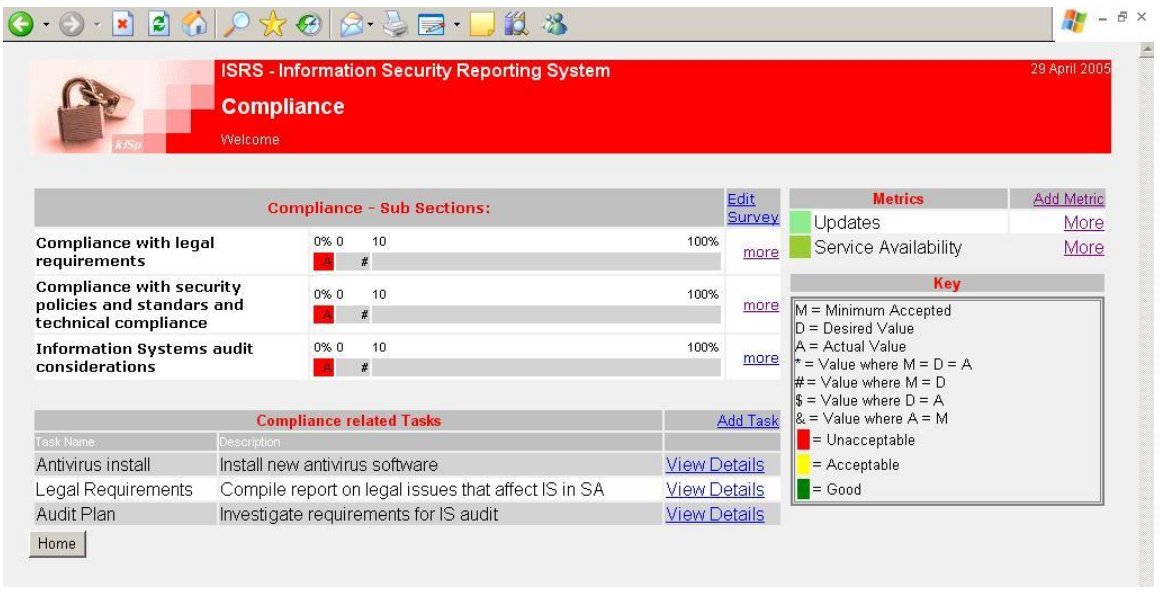


FIGURE 8.4 ISMIPS COMPLIANCE SCREEN

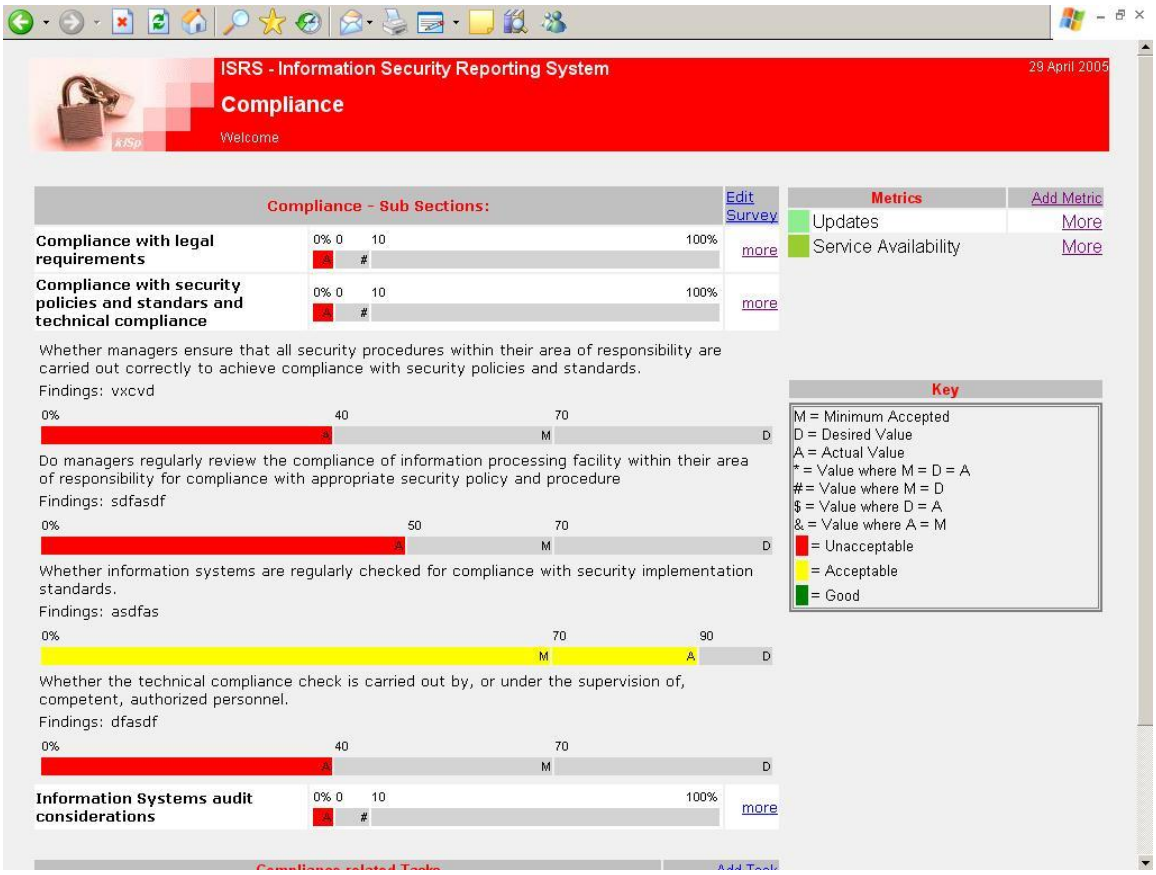


FIGURE 8.5 ISMIPS COMPLIANCE SCREEN, MORE DETAIL

Included in the table which describes metrics in the database mentioned above is an URL field. Clicking on the "more" link for each metric in the metrics table of the screen depicted in Figure 8.5 would direct the user to this URL stored in this field. The site can then make use of various visualization tools to display the information associated with that specific metric. Figure 8.6 illustrates how a simple graph can be drawn to show the history of missing updates.

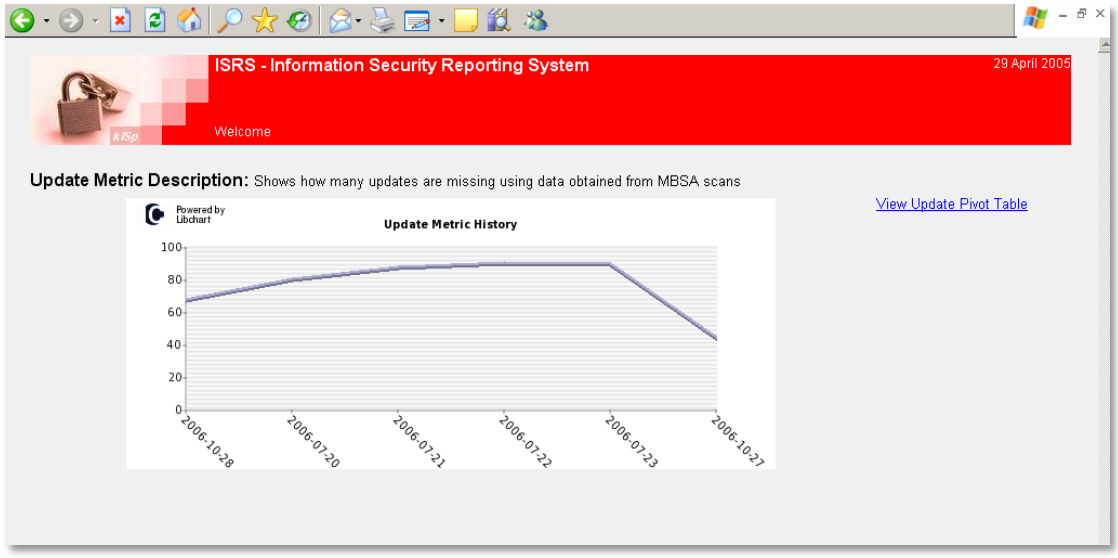


FIGURE 8.6 ISMIPS UPDATE METRIC SCREEN

A different member of the organization may only need a subset of the information provided to the CIO. The director of the human resource (HR) department may, for example, see the information depicted in Figure 8.7.

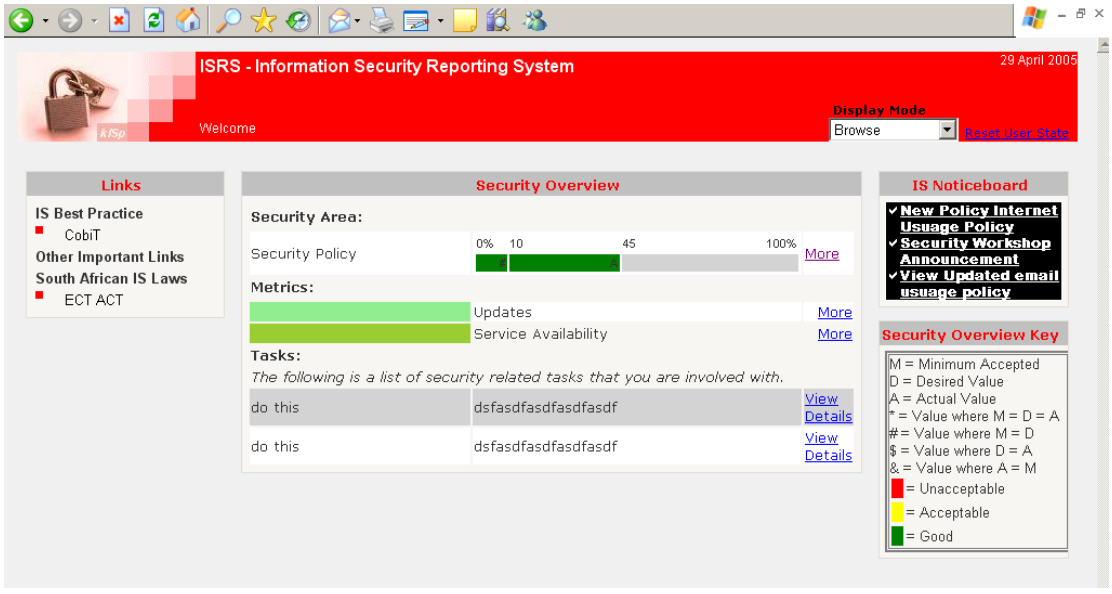


FIGURE 8.7 SAMPLE ISMIPS SECURITY OVERVIEW SCREEN FOR HR DIRECTOR

This section has demonstrated how ISMIPS may be used to make information security information visible to managers. The following section demonstrates how ISMIPS can be extended.

8.3.2 EXTENDING ISMIPS METRICS

The following demonstrates how ISMIPS could be extended to include a new metric. The ISO/IEC 27002 control number 6, Communications and Operations Management, requires that there are controls implemented to detect, prevent and recover from malicious code. The CIO, mentioned above, may want to know what initiatives and controls are in place to protect the organization against malicious software and to what extent the controls have been implemented. The board may also wish to see evidence that the situation with regard to malicious software is improving over time. Suitable metrics to measure performance in this area might be the percentage of systems with up to date anti-virus patterns installed. To accomplish this with the ISMIPS, the following will have to be done:

An anti-virus tool that is able to collect information about the percentage of systems with up-to-date anti-virus patterns installed must be selected by the company.

A web service that is able to gather the information from this tool will have to be written. This web service will have to be written to interface with the *DBAccess web service* so that the information collected can be stored in the data warehouse. The information can be stored in the generic star schema mentioned before. If this is the case, a new record will have to be added to the *fact_type* dimension. Each time the scheduler is run, the percentage of systems with latest anti-virus installed, a key linking to the appropriate date in the date dimension and a key to the appropriate *fact_type* dimension record will also have to be added to the *health_level* fact table. If necessary, a new star schema may be created in the data warehouse to store more detailed information about anti-virus statistics.

A site that will visualize the information about this metric will also have to be created.

Information about the web service that will interface with the anti-virus tool will have to be stored in the *scheduled_job* table in the operational database. The information will include the frequency that the service will have to be called, information about the service itself (e.g., execution path) and arguments that will be passed when the service is executed. This information will be used by the scheduler component to invoke the service.

Information about the metric will also have to be added as a record in the metric table of the operational database. Information would include the URL to the site created to visualize the information about the metric. In the operational database, the metric can also be associated with certain roles (so that users of a certain role will be able to see information about certain metrics) and with certain security areas. The actual health level, weighting, desired value and minimum acceptable values for this metric will then influence the overall health level of the security area that it is linked with.

With this prototype implementation of the recommended framework, it should be apparent that the type of tool that will be used to collect the data is not prescribed. Organizations will be able to choose a tool based on criteria such as their organization's budget, information needs and the preference of staff that will be responsible for working with the software. If necessary, a custom tool could be written to gather this information. The tools used to visualize the information associated with metrics are also not prescribed. As better visualization tools become available, they can be used. A variety of visualization tools can also be used with this system to visualize the same information. For example, the site that is created to visualize a certain metric may use various types of prefuse graphs to visualize the information but also link to excel pivot tables. It should be clear how flexible and scalable this prototype system is.

8.4 CONCLUSION

This chapter has described how ISMIPS has been implemented, founded on the principles outlined in FISMI. Examples of how ISMIPS can be used have also been given to more clearly demonstrate some of its features. The discussion above has shown clearly that it is possible to use FISMI to implement systems for information security management information. In addition to this, it has shown that FISMI can be used to implement scalable, interoperable systems that present information security information in a configurable, easy-to-understand and meaningful manner.

FISMI can, moreover, be used to implement affordable information security reporting systems. FISMI does not prescribe specific information security tools. Organizations, therefore, do not have to purchase expensive tools to implement FISMI. Organizations can use FISMI principles to implement a system that integrates tools that are already used by the organization to gather information security data. FISMI can also be used with open source information security tools such as OpenNMS. Likewise organizations could make use of visualization tools that they either already own or that are free to visualise the collated information security data. Properly using the SOA principles prescribed by FISMI also minimizes the costs involved with the development of the code for FISMI-based systems. Encapsulation and logic service could be reused and are easily replaced or upgraded. This has been demonstrated with ISMIPS.

Conclusion

Chapter 9

CHAPTER 9: CONCLUSION

9.1 INTRODUCTION

The previous two chapters have described the Framework for Information Security Management Information (FISMI) and the resulting prototype. This chapter concludes the dissertation by summarizing the work that has been done and describing how the research objectives set out in the introduction have been accomplished. Some of the limitations of the work are also highlighted and the opportunity for further research is discussed.

9.2 SUMMARY

This dissertation consists of eight chapters besides this concluding chapter. This section summarizes the work done in each of these chapters.

In **Chapter 1** of this work, the main and secondary research objectives were identified. The next section (9.3) discusses specifically how each of the objectives has been achieved. However, it is worth noting that the need for a framework that will facilitate the provision of effective management information in the governance of information security, in a manner that can benefit smaller organizations, was identified.

In order to more clearly understand the context in which the framework would be used **Chapter 2** briefly introduced the concepts of corporate governance, IT governance and information security governance (ISG). The need for ISG as a part of corporate and IT governance was made clear. In addition, this chapter identified role players for corporate governance, IT governance and especially ISG. It clearly confirmed that everyone in an organization, from board level down, should be involved with information security. The chapter highlighted that IT staff are not the ones who are solely or even primarily responsible for ensuring an organization's information security. The chapter also

discussed the vital role that governance frameworks and best practice standards such as CobiT and ISO 27002 play in ensuring effective ISG.

Chapter 3 discussed the information security responsibilities of various managers involved with ensuring effective information security. The importance of having the information security roles and responsibilities of all employees clearly defined and communicated was made clear. The chapter illustrated how easily the information security responsibilities for employees can be identified by using a formal process in conjunction with an information security responsibility framework and ISG best practice standards. The chapter, moreover, clearly showed that information security reporting is an important responsibility for managers at the strategic, tactical and operational levels. All of these managers should, therefore, be interested in a framework such as FISMI that makes the necessary information security information visible to all managers. In the conclusion of Chapter 3, the need for automated information security reporting tools was mentioned.

Chapter 4 described some available information security reporting tools. It showed how the need for collated information security information has been recognized and partly addressed by SIMs. The chapter, however, also highlighted that there is still a need for an affordable way of making information security information visible to all managers in smaller organizations that do not have the resources required by the commercial SIMs, like Intellitactics, that provide this facility. The value of FISMI to serve as a blueprint for automated systems that make appropriate information security information visible to various managers in a meaningful way as an aid to ISG is, therefore, clear.

Desirable characteristics of FISMI were identified in **Chapter 5.** These characteristics are summarized in Table 7.1.

Chapter 6 discussed technologies, techniques and design principles, such as web services, SOA and data warehouses that enable the development of a framework that includes desirable characteristics for the framework, such as interoperability, flexibility and adaptability.

The above-mentioned chapters showed that FISMI was not only desirable but also possible to achieve. **Chapter 7** described FISMI, a Framework for Information Security Management Information. The chapter described how the technologies, techniques and design principles identified in Chapter 6 were used in FISMI to accomplish the desired characteristics identified in Chapter 5. The chapter also highlighted how FISMI could help managers accomplish some of their ISG responsibilities highlighted in Chapter 3.

To motivate the feasibility of implementing FISMI, **Chapter 8** described the prototype system built based solidly on FISMI.

9.3 RESEARCH OBJECTIVES

In the introduction to this dissertation, the primary objective of this project was identified as the development of a framework that would facilitate the provision of effective management information in the governance of information security. The framework would be developed in such a manner that it can be used by smaller organizations with limited resources. In order to accomplish this, four secondary research objectives were identified:

1. To compile a set of desirable characteristics of a framework to facilitate the provision of effective management information in the governance of information security;
2. To analyse which techniques and technologies are well suited for use in the framework;
3. To motivate that the framework can be used in smaller organizations with limited resources;
4. To develop a prototype system based on the framework as proof of concept.

These objectives have been achieved in the following manner:

Secondary objective 1: Chapter 5 identified a list of desirable characteristics of a framework to facilitate the provision of effective management information in the governance of information security. These characteristics are summarized in Table 7.1.

The list was compiled by studying some characteristics of security information management (SIM) tools, management information systems (MISs), decision support systems (DSSs), executive dashboards, compliance dashboards and continuous auditing tools. The characteristics listed in this chapter would be desirable for any ISG reporting tool, whether it is designed for use in either big or small organizations.

Secondary objective 2: Chapter 6 of this dissertation showed that by applying SOA, data warehousing and portal principles and using good visualization tools, many of the desirable characteristics of FISMI can be achieved. Each of these technologies, techniques or design principles were described. How they can be used to achieve some of the desirable FISMI characteristics was then clearly shown. Tables 6.3; 6.5; 6.6 and 6.7 summarize this.

Secondary objective 3: The conclusion of the previous chapter motivated why FISMI can be used by smaller organizations with limited resources. FISMI does not prescribe the use of expensive tools to gather information security data. Organizations can use existing or open source tools that gather information security data. The eases of code reuse, upgrade and redesign associated with the application of SOA principles in FISMI also allow for cost effective system design.

Secondary objective 4: A prototype system called ISMIPS has been designed to prove the FISMI concept. Chapter 8 describes the prototype. The prototype was implemented based firmly on FISMI. It demonstrates that FISMI can be implemented.

Primary objective: *the development of a framework that will facilitate the provision of effective management information in the governance of information security for organizations with limited resources***.** This work has established the need for such a framework. FISMI accomplishes this objective. Chapter 7 clearly explains the characteristics of FISMI that make it an acceptable solution. And as mentioned above, the prototype system shows that FISMI can be implemented. In addition, the principles have been presented at the Human Aspects of Information Security and Assurance (HAISA) Conference, an international conference in Plymouth, England. A copy of the article that

was peer-reviewed, accepted and presented at this conference is listed as Appendix 1 of this dissertation.

9.4 FURTHER RESEARCH

As was discussed in the introduction, there are various areas of interest that have not been addressed in this work. These present interesting areas for further research.

This dissertation has not provided an implementation methodology for FISMI. As was explained in Chapter 7, FISMI is more than just a blue-print for a software reporting tool. It encourages managers to carry out information security activities such as deciding on an information security standard, completing questionnaires to assess information security status, determining acceptable and desirable levels of performance for security areas and determining effective metrics. This work has not provided any suggestions about how such tasks can be achieved. Although providing evidence for the value of using SOA principles and showing that they can be used effectively, this work has not addressed issues around the implementation of these principles. For example, the issue of web service security is not addressed. Similarly, although the value of using a data warehouse with the framework has been highlighted, details about how the data warehouse will be implemented have not been addressed. These are a few of the interesting topics which could be considered when doing further research into an implementation methodology for FISMI.

Converting the prototype system, as described in Chapter 8, into a fully functional system and testing it within an organization would assist in developing an implementation methodology for FISMI and would further prove the framework's feasibility.

9.5 CONCLUSION

Information security is an extremely interesting and ever-changing field. Ensuring proper ISG in any organization can also be a daunting task. Managers without information technology skills may feel especially apprehensive about having information security

responsibilities. Clearly defining and communicating these responsibilities to managers will make ISG more achievable. Providing these managers with information resources needed to see how they are performing and where improvement is needed will also make their information security tasks more manageable. This dissertation has presented a framework that can be used to support managers in ensuring ISG. The framework can be used effectively in small or large organizations. It is affordable, scalable, distributable and interoperable and can be used to effectively present appropriate meaningful information security information to different managers.

APPENDIX A

PAPER PRESENTED AT HAISA 2007

An Information Security Reporting Architecture for information security visibility

M. Viljoen[1], R. von Solms[2] and M. Gerber[3]

Centre for Information Security Studies, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

[1]s20310694@nmmu.ac.za, [2]rossouw@nmmu.ac.za, [3]Mariana.Gerber@nmmu.ac.za

Abstract:

The importance of information in business today has made the need to properly secure this asset evident. Information security has become a responsibility for all managers of an organization. To better support more efficient management of information security (IS), timely IS information should be made available to all managers. This paper discusses an Information Security Reporting System Architecture that aims to improve the visibility and contribute to better management of IS throughout an organization by enabling the provision of summarized, comprehensive IS information to all managers.

Key words:

Information security, information security reporting architecture, information security visibility, information security management.

Introduction:

Information has and will continue to be seen as an extremely important asset in today's business environment (Business Link, 2006; Ernest & Young, 2006). It is, therefore, important that an organization recognizes the critical need to properly protect and secure its information like it would any other valuable asset, for example, its financial assets (Business Link, 2006; ISO, 2006). It is also important that every member of the organization recognize that they play a role and share responsibility for the organization's information security (IS). This is especially true of managers who are responsible for directing and controlling the assets that they are answerable for (Whitman and Mattord, 2004). If every member of an organization is to be able to have a share in information security it follows that every person, and especially managers in the organization, should have access to relevant information about the organization's IS. It is therefore important that the appropriate IS reports are available to people at all levels of an organization.

Today there are dozens of tools that can be used to gather and report on IS information (Insecure.org, 2006). Each of these tools has their different strengths and weaknesses but no single tool is able to completely report on all information security concerns to all levels of the organization. It is, therefore, often difficult for management to see the big picture with regard to information security (B. Robison, 2005).

The objective of this article is to describe and motivate an architecture that makes use of existing network monitoring and reporting tools to enable reporting of IS information to all levels of an organization. This architecture should enable the organization to have available a customizable, summarized and comprehensive overview of information security. It should enhance the visibility of information security in the organization and should assist managers at different levels of the organization to direct and control appropriate information security initiatives more effectively. A prototype has been developed, based on the recommended architecture, as a proof of concept. The prototype system is called the Information Security Reporting System (ISRS). The recommended architecture is referred to as the ISRS architecture.

Before beginning with the description of the architecture, some desirable characteristics for an ISRS architecture that supports efficient information security management will briefly be discussed.

Desirable characteristics for ISRF

Managers have the responsibility for directing and controlling the individuals and assets under them in an organization. They will direct (let people know what they have to do) and control (make adjustments as it becomes necessary) these assets in a way that will enable the organization to meet its objectives (Marchewka, 2003). One of the important objectives of an organization should be information security (Whitman and Mattord, 2004). Information security is such an important concern that in many countries a failure to demonstrate due diligence may lead to legal liability (Frazer, 2005; Whitman and Mattord, 2004). Managers should therefore accept

responsibility for directing and controlling information security concerns under their sphere of influence. As mentioned above, this is true for managers at all levels of the organization. This includes: staff like CIO, CISO, network and system administrators who work directly with information technology or information security; members of the board and board committees that are responsible for the governance of the organization and managers of other departments of the organization (Corporate Governance Task Force, 2004). The corporate governance task force recommends that there should be a manager in each organizational unit responsible for information security concerns under the control of that organizational unit. They contend that management responsibilities include conducting risk assessments for their units, implementing policies and procedures and testing that information security controls and techniques are being implemented properly for their unit (Corporate Governance Task Force, 2004). If managers are going to have these responsibilities it follows that they should be equipped with IS information. An architecture that effectively facilitates the reporting of this information will include some of the desirable characteristics mentioned below.

A good reporting system should be configurable to meet the needs of the different mangers (McLeod, 1983; Corporate Governance Task Force, 2004). Different managers will have different responsibilities and amounts of influence when it comes to information security. For example a manager in the human resource department, a manager in the information technology department and the CEO of an organization are all going to have different responsibilities, amounts of influence and interest in information security. It is therefore important that each manager receives IS information that pertains to that manager.

Furthermore, it would be of great value if the relevant information for a particular user is presented in a manner that is easy to understand and shows the state of IS as a whole or the state of a particular IS concern at a glance (Few, 2006). This will assist managers to take corrective.

An ISRS architecture will also be of value if it assists managers to measure how well they comply with internationally accepted IS standards. Standards and policies are essential for the proper management of information security (Whitman and Mattord, 2004; Purser, 2004). Security standards, such as ISO/IEC 17799, prove invaluable in helping managers at the governance level to define information security goals, organizational information security standards and effective management practices (ISO, 2005). It is also valuable for information security policy development.

It would, moreover, be desirable if the ISRS is highly extensible, flexible and adaptable (Ackoff, 1967). It should allow for different tools to be easily integrated with the system. Although security standards, such as ISO/IEC 17799, will provide general guidance, each organization is different, and will make use of different tools and technologies to implement their information security controls. The amount of money that an organization has to spend on information security alone will cause different organizations to have tools and systems that differ widely. Today there are dozens of tools that can be used to gather and report on IS information (Insecure.org, 2006).

Insecure.org mentions some of these such as SNORT, Nessus, NetStumbler, Nmap, MBSA. As mentioned before, each of these tools have their different strengths and weakness but no single tool is able to completely report on all information security concerns to all levels of the organization. This often makes it difficult for management to see the big picture with regard to information security. Advances in technology will also undoubtedly lead to the development of new and improved monitoring and reporting tools that make new IS information available. There are also organizations that have IS tools that have been custom written for them. The challenge is therefore to develop an architecture where different tools and modules can easily interface with each other as the need arises to gather information from these different tools and to present it in a useful manner.

It would be beneficial to have an architecture that is scalable and supports large or small heterogeneous distributed environments. Many organizations today have IT infrastructures that incorporate different platforms. For example it is not uncommon for one organization to run Windows and UNIX operating systems. There is also a lot of work being done in the area of distributed computing. An architecture that allows for interfacing across platforms to gather and report on IS information would therefore be of great value.

Another Desirable characteristic of an ISRS is that it will facilitate new ways of correlating and analyzing data (Bhalala, 2007). It would be useful to pull together information gathered by different tools with different file formats and application programming interfaces such as SNORT, Nessus, NetStumbler, Nmap, MBSA in such a way that allows one to find new relationships between the information from each tool, show the history of the specific information gathered, do new forms of analysis on the combined information.

In summary it can be said that the desirable characteristics for ISRS architecture should include that it will be standards based, highly extensible, distributable and show the overall, summarized state of information security at a glance.

In the following section an ISRS architecture will be described as an envisioned solution that includes these desirable features.

ISRS Architecture

An ISRS architecture has been designed to incorporate the desirable features described above. A prototype system based on this architecture has been developed to test and demonstrate the feasibility of an ISRS that integrates information from different toolsets, and makes it visible to managers at different levels of an organization.

In developing the ISRS architecture the assumption was made that the best approach for an organization would be to link all their information security initiatives to controls specified by best practice standards such as BS ISO/IEC 17799 or CobiT. Every control, or security area, is linked to a set of key performance indicators that are used to indicate the measure of compliance with that control. The key performance indicators can be grouped into the following categories: survey results, the progress of tasks or activities, and metrics. The overall health of a control is determined by using weights and values associated with the survey results, tasks and metrics associated with that control. The relationships between controls and key performance indicators are stored in an operational database. The operational database also stores relationships between people or user roles and controls and/or key performance indicators.

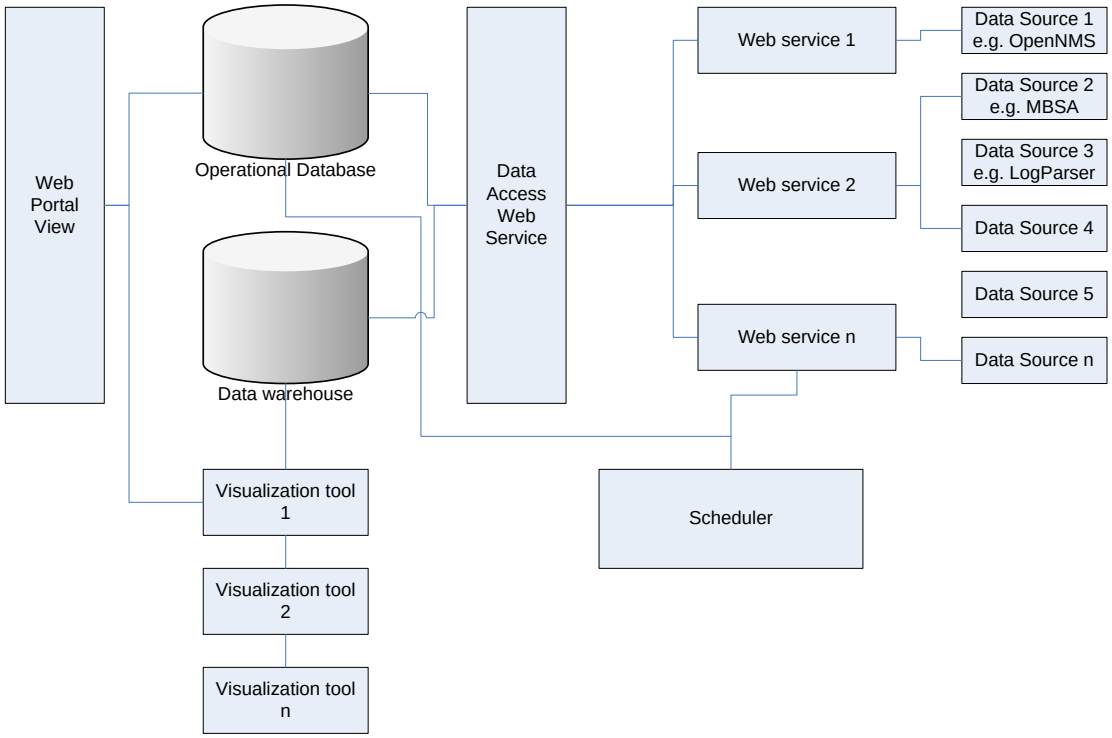
There are several benefits associated with this approach. This approach provides the managers of the organization with a standards-based way of considering IS. Associating data collected with a limited number of clearly defined controls with a single overall health level associated with each control makes it easy display a summarized view of the level of compliance with controls in a simple clear manner. It also facilitates the ability to drill-down to more specific information. Being able to link different people in an organization to different controls, security tasks and metrics means being able to customize which IS information is displayed to different people.

Another desirable characteristic of an ISRS is that it will facilitate new ways of correlating and analyzing data. To meet this objective the ISRS architecture makes use of a data warehouse to store the IS information gathered. Within the data warehouse there is a general purpose star schema that can be used to store the general information about metrics. If this general purpose schema does not meet the needs of the metric and information that has to be stored in relation to it another star schema will have to be added to the warehouse. Data warehouses are designed especially so that this type of analysis and can be done efficiently and easily to improve decision support (Kimball and Ross, 2002).

Yet another desirable characteristic of a good ISRS is that it should be extensible and distributable. The ISRS architecture allows for a system that would accomplish this by making use of a service oriented architecture approach. Figure 1.2 depicts the components of the ISRS architecture as described below. ISRS architecture makes use of web services to interface with and retrieve certain information from existing monitoring and reporting tools. A Data Access web service is used to write the information to a data warehouse and to access information from the warehouse and operational database. A scheduler queries the operational database for a list of jobs (web service functions) that it must run and information pertaining to the running of these jobs. It then makes the necessary calls to the web services that encapsulate the monitoring and reporting tools. Web service interfaces to various visualization tools can be plugged in to facilitate the visualization of the information stored in the data warehouse. The use of web services to encapsulate existing tools has a number of advantages. Different organizations may for many reasons have a wide array of monitoring tools that collect IS information running in their systems. With this architecture, when a new tool becomes available it is easy to retrieve the information it exposes by writing a new web service that can interface with the tool or make use of an existing web service. Which web service should be called, how often this should be done and other

information to do with the invocation of this service must then simply be added to the operational database from where the scheduler will retrieve it and invoke the service. The service will in turn have the responsibility of interfacing with the data access web service to store the data in the appropriate place in the data warehouse. As can be seen this approach to gathering information is very extensible because new tools and the metrics associated with these tools can easily be integrated into the system as the need arises. Web services are commonly used to provide a standard way of remotely invoking functionality across different platforms (Kalani and Kalani, 2003, p 288-290). This makes the framework highly scalable and flexible since it means that the different tools and web services used can either all be located on a single machine, or they can exist on different virtual machines on one a single physical machine, or they can be distributed across the infrastructure of an organization.

Figure 1.2 – Components of ISRS architecture.



The prototype system, ISRS, demonstrates how this architecture can be implemented. To promote a better understanding of the practical value of the ISRS architecture and how it can be implemented to incorporate the desirable characteristics discussed earlier the prototype system will now be discussed.

Prototype description

As mentioned above the assumption was made that the best approach for an organization would be to link all their information security initiatives to controls specified by best practice. ISRS, therefore, has a survey component that is based on the SANS Audit Checklist compiled by the SANS institute (Thiagarajan, 2006). The checklist is based on the BS ISO/ IEC 17799:2005 standard. This checklist consists of 11 main categories. These categories are used as security areas or controls in the current prototype implementation of the ISRS architecture.

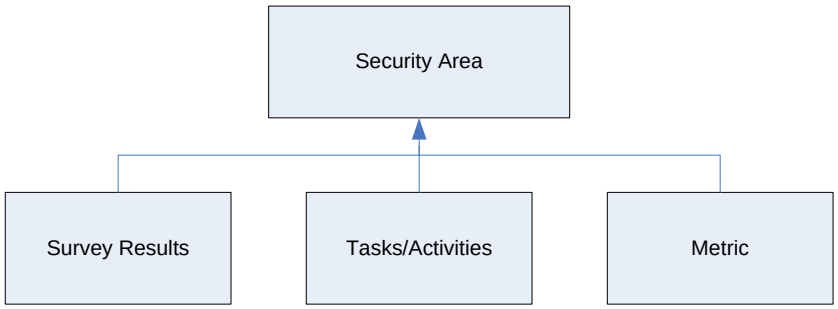
Each security area has a number of questions (based on the SANS audit checklist) related to it. Each of these questions can be assigned a weighting to indicate the level of importance that the company assigns to that question. The question also has three other important attributes associated with it. These are: The “min acceptable” value. This value indicates the minimum percentage of compliance that is accepted by that company for that specific question. The “desired value” to indicate to what level the company would like to have compliance with the question. The “actual value” which indicates to what extent the company is complying with the question. Managers, possibly at the board level, will have to assign individuals with the required knowledge to answer these questions. This can be done by creating a task in ISRS.

The progress a task will affect the health level of the security area that it is related to. The task progress is updated by users to reflect whether the tasks progress is *acceptable*, *good* or *unacceptable*. A task is also classified as critical or not.

A security area can have security metrics associated with it. A metric can be gathered by means of available tools, modules or by audit/survey components. To illustrate: A metric could be percentage of updates completely installed on machines in an organization. The information for this metric can be collected from tools like MBSA and Nessus by means of web service based modules. A metric could be the percentage compliance with the organization’s physical security policy and information for this metric could simply be collected from a completed online questionnaire. Like the questions from the SANS audit checklist, a metric has “min acceptable”, “desirable” and “actual values” associated with it.

The ability for appointed managers to be able to set the weightings, *“min acceptable” and “desired”* values for security areas and all key performance indicators should contribute to the manager’s ability to direct IS initiatives. When the actual value is visualized in relation to the *“min acceptable” and “desired”* values, it should be simple for the manager to see where corrective action is necessary thereby assisting him to exercise necessary control.

Figure 1.1 Categories of key performance indicators that are linked to security areas in the current prototype implementation of the ISRS architecture.



The initial prototype system has a web interface created in asp.net. This component of ISRS is referred to as the ISRS web interface.

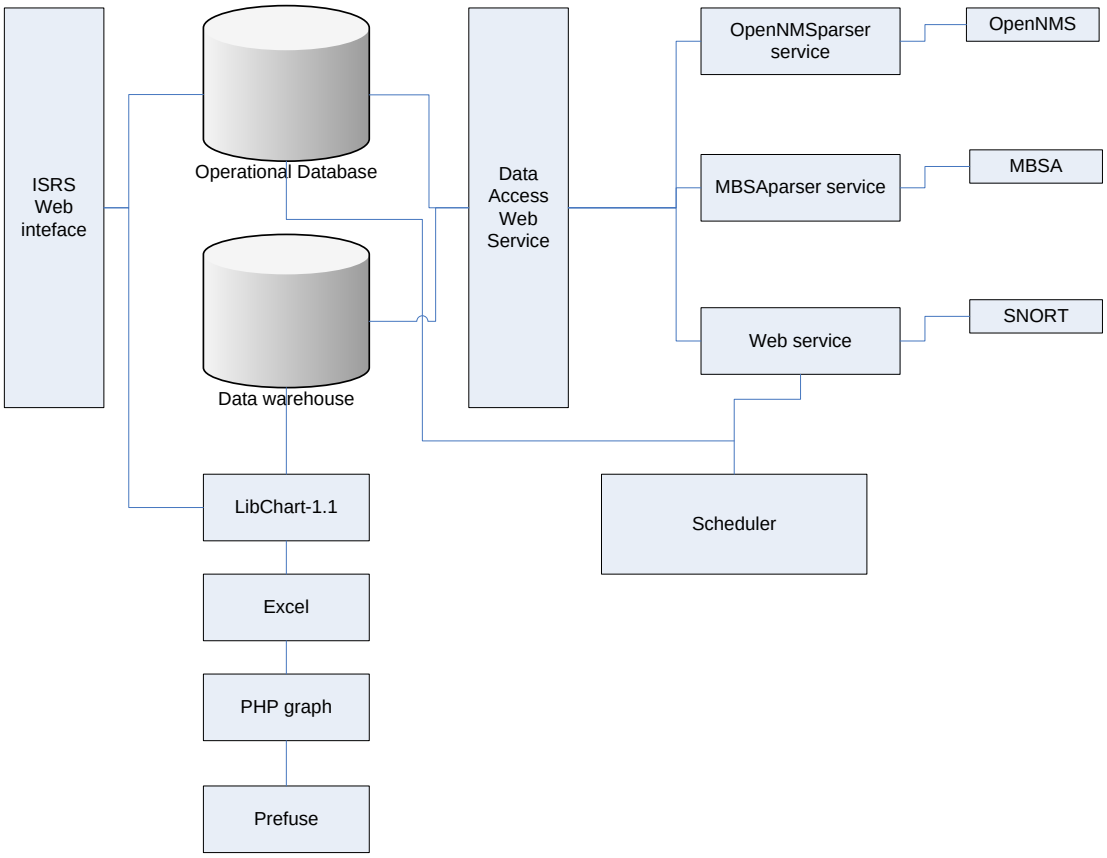
Both the operational database component and the data warehouse component of the ISRS architecture have been implemented as postgres databases.

There is also a web service, called the DBAccess service, that is responsible for interfacing with the data warehouse and the operational database.

The initial prototype system has web services that interface with MBSA and OpenNMS. The web service, MBSAparser service, which interfaces with MBSA, collects information gathered by the MBSA software about updates on the network. This information is written into a star schema in the data warehouse. The web service that interfaces with openNMS, the OpenNMSparser service, similarly retrieves information that is gathered by OpenNMS about service availability and writes that to a star schema in the data warehouse.

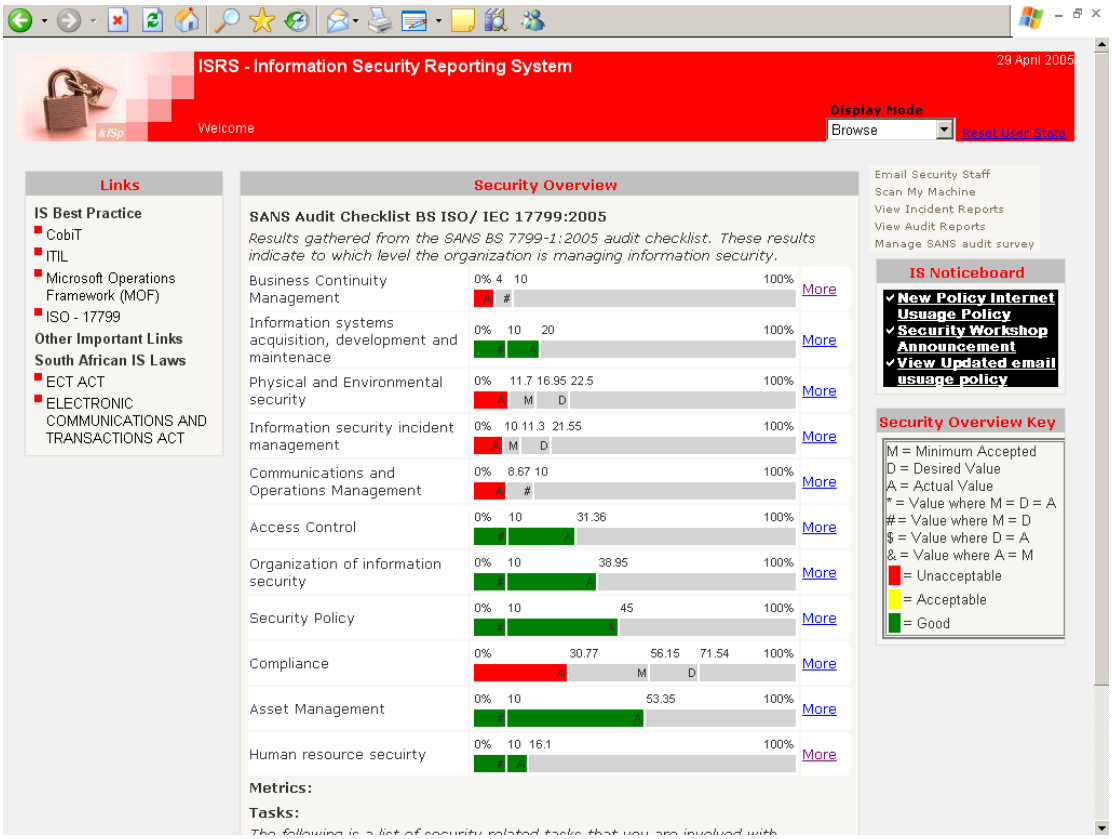
The scheduler service is the software component that uses the information in the Scheduled_jobs table in the operational database to invoke the execution of the web services that interface with the data collection.

Figure 1.3 – Components of an ISRS prototype system.



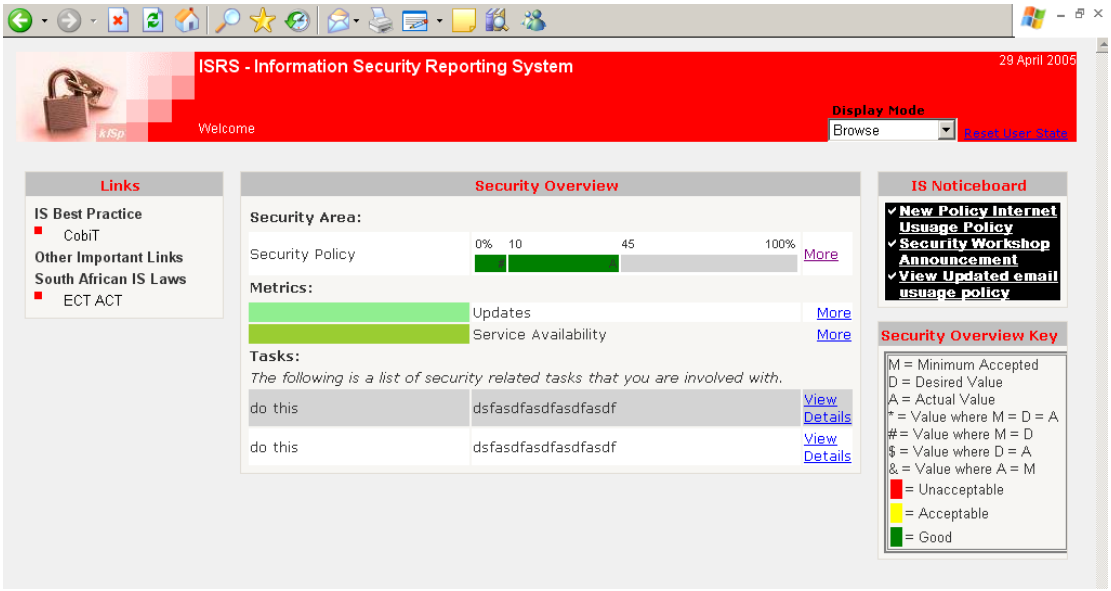
As mentioned earlier, the operational database maps specific users to roles and roles to metrics and security areas. Roles will also have links, and news associated with them. With these mappings each user that logs on to the system will be able to see only the information that applies to him. Figure 1.4 below illustrates a screen that a member of the board of a company may see. As can be seen in Figure 1.4 the health level of each security area should be clearly visible based on the minimum acceptable, desired and actual values for each security area. This health level is calculated by a service that is run regularly by the scheduler component. This calculation is made based on the actual values, weightings, and minimum and desired values for tasks, survey results and metrics linked with that security area in the operational database. The board member is likely to want to see the health of all security areas in the organization.

Figure 1.4 – Main page of ISRS web interface as viewed by member of the board.



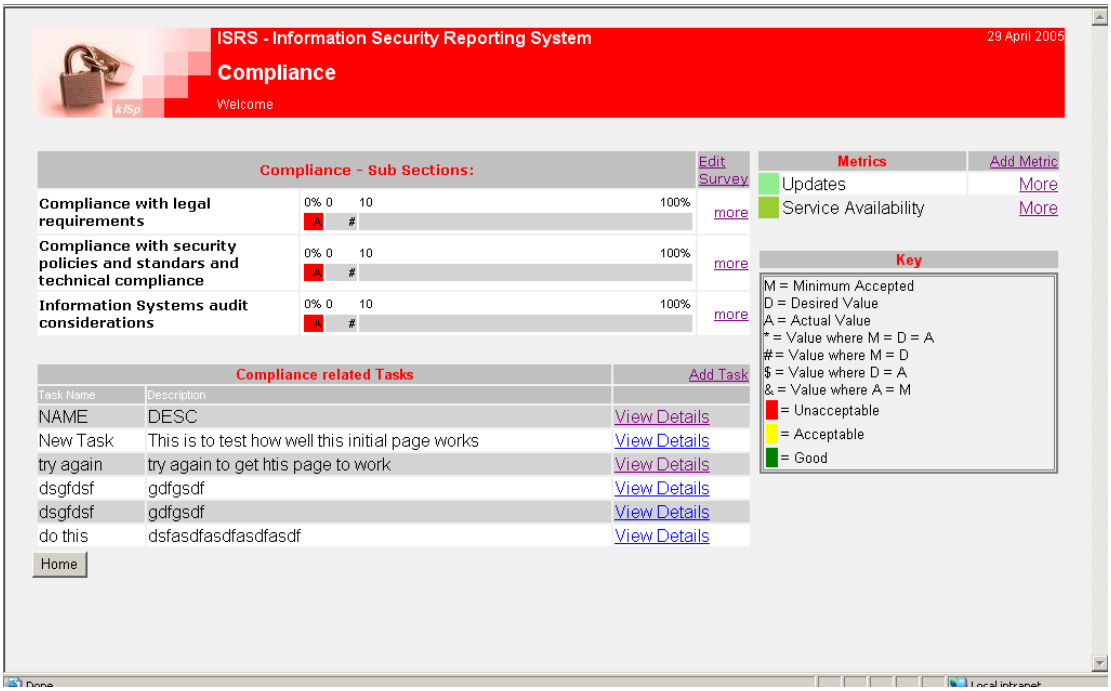
A different member of the organization may only need a subset of the information provided to the board member and may see a screen more like the one depicted in figure 1.5 below.

Figure 1.5 – Main page of ISRS web interface as viewed by a manager who only needs a subset of the information that the board member would receive.



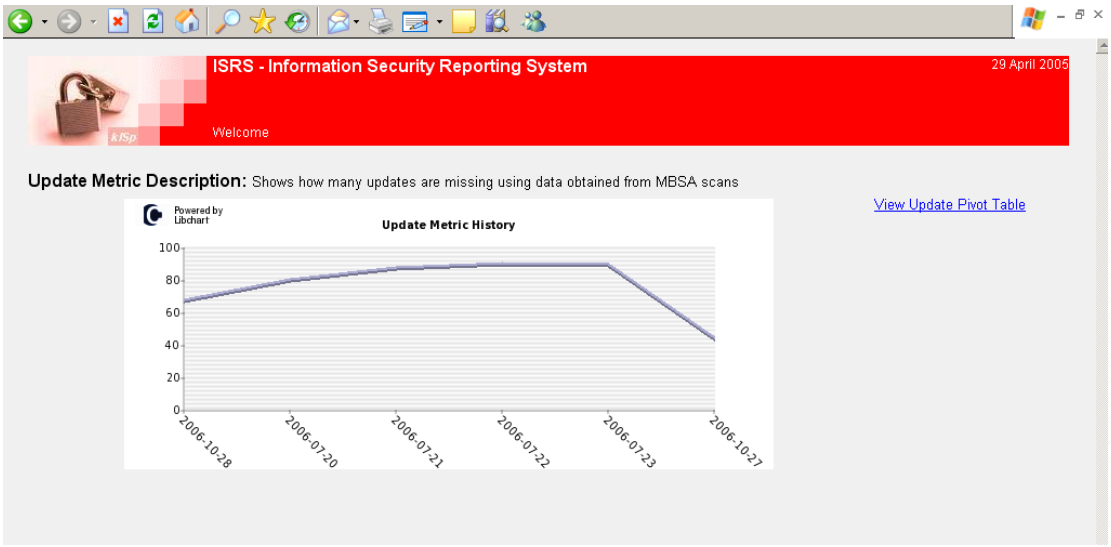
From this initial screen users will be able to drill down to get detailed information. For example if a member of the board who is logged on and sees the screen depicted in figure 1.5 decides that he would like to know why the health level of the compliance security area is rated as unacceptable, he could simply click on the *more* link of the compliance security area. The user would then see a screen like the one depicted in figure 1.6 below with ISRS.

Figure 1.6 – Page that allows one to drill-down into more specific information about the compliance security area.



A field that stores a URL to a site responsible for visualizing the information collected about a metric is stored in a table in the operational database. Clicking on the *more* link for a metric (refer to Figure 1.6) would direct the user to the URL stored in this field. The site can then make use of various visualization tools to display the information associated with that specific metric. Figure 1.7 illustrates an example of how a simple graph can be drawn to show the history of missing updates.

Figure 1.7 – Example of a visualization site for a specific metric.



The following illustrates how this system could be extended to include a new metric. The ISO 17799 control number 6, Communications and operations management mandates controls to detect, prevent and recover from malicious code. A member of the board may want to know what initiatives and controls are in place to protect the organization against malicious software and to what extent the controls have been implemented. The board may also wish to see evidence that the situation with regard to malicious software is improving over time. Suitable metrics to measure performance in this area might be the percentage of computers with up to date anti-virus patterns installed. To accomplish this with the ISRS system the following will have to be done:

An antivirus tool that is able to collect information about the percentage of systems with up to date antivirus patterns installed must be selected by the company.

A web service that is able to gather the information from this tool will have to written. This web service will have to be written to interface with the DBAccess web service so that the information collected can be stored in the data warehouse. The information can be stored in the generic star schema mentioned before.

A site that will visualize the information about this metric will also have to be created.

Information about the web service that will interface with the antivirus tool will have to be stored in the scheduled_job table in the operational database. This information will be used by the scheduler component to invoke the service.

Information about the metric will also have to be added as a record in the metric table of the operational database. Information would include the URL to the site created to visualize the information about the metric. In the operational database the metric can also be associated with certain roles (so that users of a certain role will be able to see information about certain metrics) and with certain security areas. The actual health level, weighting, desired value and minimum acceptable values for this metric will then influence the overall health level of the security area that it is linked with.

With this prototype implementation of the recommended framework it should be apparent that the type of tool that will be used to collect the data is not prescribed. Organizations will be able to choose a tool based on factors such as their organizations budget, information needs, and preference of staff that will be responsible for working with the software. If necessary a custom tool could be written to gather this information. A variety of visualization tools may be used. As better visualization tools become available they can be used. It is also possible that tools that are used to gather the information are dashboard type tools or have custom ways of visualizing the data they collect. ISRS can simply link to the tool's own visualization display as a drill-down option. The metrics that are to be used are also not prescribed. Although suggestions can be made on which metrics should be implemented with the implementation of the ISRS architecture, these recommendations are beyond the scope of this article. In a similar way, although suggestions can be made as to the weightings that should be assigned to various security areas or metrics these are not prescribed by the ISRS architecture. Managers are rather allowed to set or adjust the recommended weightings, minimum acceptable and desired levels to suite the needs of their specific organization. It should be clear how flexible and scalable this prototype system is.

Conclusion

The ISRS architecture has several features that make it a desirable approach to follow when implementing an ISRS to improve visibility of information security in the organization and to use as a means to aid in better management of information security throughout an organization.

By following a standards-based approach and making use of technologies such as web services, data warehouses, operational databases and visualization tools the architecture should be able to enhance the visibility of information security in the organization. It should also allow for a customizable, summarized and comprehensive overview of IS concerns to managers. This should in turn help managers to direct and control IS concerns more efficiently. The principles of service oriented architecture applied in the design of the architecture also make the ISRS extensible, flexible and distributable.

References:

Business Link. (2006). Information security best Practice [Online]. URL http://www.businesslink.gov.uk/bdotg/action/printguide?r.l1=1073861197&r.l3=1075406921&topicId=1075406921&r.t=RESOURCES&r.i=1075406928&r.l2=1075408323&r.s=pg

Whitman, M.E., Mattord, H.J. (2004). Management of information security. Canada: Thomson course technology.

Insecure.org (2006). Top 100 network security tools. [Online] URL http://sectools.org/

Robison, B. (2005). Security dashboard - Are high-level views the answer to getting managers the cybersecurity status information they need to make decisions? [Online] URL http://www.fcw.com/article91327-11-07-05-Print#related

Kalani, A., Kalani, P. (2003). MCAD/MCSD Developing XML Web Services and Server Components with Visual C# .NET amd Microsoft .NET Framework. USA: Que Publishing.

Marchewka, J.T. (2003). Information technology project management. Providing Measurable Organizational value. USA: John Wiley & Sons.

Frazer, A. (2005). Sarbanes-Oxley Compliance Journal. Due Diligence risks in network security. [Online] URL http://www.s-ox.com/Feature/detail.cfm?articleID=1148

Corporate Governance Task Force. (2004). Information security governance: a call to action [Online]. URL http://www.cyberpartnership.org/

ISO. (2006). ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management [Online]. URL http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

Purser, S. (2004). A practical guide to managing information security. [Online] URL http://books.google.co.za/books?id=mczgkqHSIXUC&dq=why+are+information+security+standards+so+important&pg=PA147&ots=uY2Zws5uD4&sig=--T3VZUI0Fg4fir6vsc-9MmsztU&prev=http://www.google.co.za/search%3Fhl%3Den%26q%3Dwhy%2Bare%2Binformation%2Bsecurity%2Bstandards%2Bso%2Bimportant%26meta%3D&sa=X&oi=print&ct=result&cd=2#PPR9,M1

Thiagarajan, V. (2006). SANS Audit Checklist. [Online] URL http://www.sans.org/score/checklists/ISO_17799_2005.pdf?portal=f36013c72bc89932f16f84f4f89245dc

McLeod, R. (1983). Management Information Systems second edition. USA: Science research associates, inc. Pages 40 – 46

Frew, S. (2006). Information Dashboard Design: The effective visual communication of data. Page 50

Ackoff, R. (1967). Management Misinformation Systems, Management Science.

Bhalala, M. (2007). Compliance Dashboards for regulated industries, Quality Digest Magazine. [Online] URL http://www.qualitydigest.com/aug06/articles/03_article.shtml

REFERENCES

Ali, S. (2006). Effective Information Technology Governance Mechanisms: An Australian study. *Gadjah Mada International Journal of Business* , 69-102.

Bassett, J. (2007, June). Security in management's terms. (R. Filipek, Ed.) *Internal Auditor* , 27-31.

Batchelor, R. (2005, October). Executive Dashboard: a decision maker's favourite. *Franchising world* , 27-31.

Brandt, D. (2007, August). SOA Explained. *Contol Engineering* , 22.

Broadbent, G., & Elli, M. (2006, December). ISO 17799: Standards for Security. *The Information Management Journal* , 43-52.

Brotby, K. (2007). Information security governance: Who needs it? *Information systems Control Journal , 2*, 13-14.

Brown, W. C. (2006). IT governance, architectural compentency, and the Vasa. *Information management & computer security* , 140-154.

Burgert, P. (2004, April 26). Red Alert for Chief Executives: Make Cyber Security a Priority. *American Metal Market* , p. 37.

Business Wire. (2005, October 19). Authentic metrics provide a practical answer to the question asked everyday: "Are we secure?". *Business Wire* . New York, USA: Gale Group.

Bussiness Link. (2006). *Information Security Best Practice*. Retrieved February 2007, from http://www.businesslink.gov.uk/bdotg/action/printguide?r.l1=1073861197&r.l3=1075406921&topicId=1075406921&r.t=RESOURCES&r.i=1075406928&r.l2=1075408323&r.s=pg

Bussiness Wire. (2008, April 1). Intellitactics partners will cash in on services for the SIEM channel. *Business Wire* .

Carbonel, J.-C. (2008). Assessing IT security governance through a maturity model and the definition of a governance profile. *Information Systems Control Journal , 2*, 29-32.

Carr, J. (2007, September 1). *The SIM solution*. Retrieved May 23, 2008, from SC Magazine: http://www.scmagazineus.com/The-SIM-solution/article/35618/

Chartered Accountants of Canada. (1999). *Continuous auditing - 1999 - Executive Summary*. Retrieved July 29, 2008, from Chartered Accountants of Canada: http://www.cica.ca/9/8/9/index1.shtml

Chou, L. Y., Du, T., & Lai, V. (2007). Contionuous auditing with a multi-agent system. *Decision Support Systems , 42*, 2274-2292.

Compliance Home. (2007, November 29). *FISMA News*. Retrieved May 23, 2008, from Compliance home: http://compliancehome.com/news/FISMA/11832.html

Compliance Home. (2007, December 12). *HIPAA News*. Retrieved May 23, 2008, from Compliance Home: http://compliancehome.com/news/HIPAA/11911.html

Congress of United States of America. (2002). *The Sarbanes Oxley Act of 2002.* Retrieved October 4, 2007, from http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf

Corporate Governance Task Force. (2004). *Information Security Governance - A Call to Action.* National Cyber Security Summit Task Force.

De Haes, S., & Van Grembergen, W. (2008). Practices in IT Governance and Business/IT Alignment. *Information Systems Control Journal , 2*, 23-27.

Deam, J., Rathbone, G. A., Waite, M., & Manser, M. H. (1984). *VIA Afrika learner's dictionary.*

Deitel, H. M., Deitel, P. J., Listfield, J., Nieto, T. R., Yaeger, C., & Zlatkina, M. (2002). *C# how to program.* Upper Saddle river, New Jersey, USA: Prentice-Hall, Inc.

Dodds, R., & Hague, I. (2004, December). Information Security - More than an IT Issue? *Chartered Accountants Journal* , 56-57.

Dubie, D. (2008). *Guide to information security management. Security-information market continues to flourish.* Retrieved May 23, 2008, from PC World: http://www.pcworld.com/businesscenter/article/144638-3/securityinformation_market_continues_to_flourish.html

Dubie, D. (2008). *Guide to security information management. Best practice for successful SIM deployment.* Retrieved May 23, 2008, from PC World: http://www.pcworld.com/businesscenter/article/144638/guide_to_security_information_management.html

Edwards, J. (2008, January 17). *The 10 best free security tools*. Retrieved May 19, 2008, from IT Security: http://www.itsecurity.com/features/10-best-free-security-tools-011708/

Erl, T. (2004). *Service-Oriented Architecture: a field guide to integrating XML and web services.* Upper Saddle River, New Jersey, USA: Prentice Hall PTR.

Fitzgerald, K. J. (1994). Establishing security in a multi-platform, multivendor, enterprise-wide IT environment. *Information management & computer security , 2* (4), 9-15.

Flowerday, S., Blundell, A., & Von Solms, R. (2006). Continuous auditing technologies and models: A discussion. *Computers and security , 25*, 325-331.

Fogarty, K. (2004). The governing concepts of governance. *Baseline* , 79.

Fowler, F. G., & Fowler, H. W. (1969). *The pocket Oxford Dictionary of current english* (Fifth Edition ed.). Oxford, Great Britain: Oxford University Press.

Frazer, A. (2005). *Due dilligence risks in network security*. Retrieved March 2007, from Sarbanes-Oxley Compliance Journal: http://www.s-ox.com/Feature/detail.cfm?articleID=1148

Freeman, E. (2007). Holistic Information Security: ISO 27001 and Due Care. *Information Systems Security , 16*, 291-294.

Garver, R. (2005). The Move oward Service-Oriented Architectures. *American Banker , 170* (142), p14ET-15ET.

Grance, T., Stevens, M., & Myers, M. (2003). *NIST Special Publication 800-36. Guide to Selecting Information Technology Security Products.* National Institute of Standards and Technology, Computer Security Division. Gaithersburg: Information Technology Laboratory.

Green, M. (2006, August). Businesses look to continuous auditing, monitoring. *Best's Review* . AM Best Company Inc.

Hartman, B., Flinn, D. J., Beznosov, K., & Kawamoto, S. (2003). *Mastering Web Services Security.* Indianapolis, Indiana, USA: wiley Publishing, Inc.

Hitachi ID Systems. (2008). *Hitachi ID products*. Retrieved May 20, 2008, from Hitachi-id.com: http://hitachi-id.com/products/

Hofstader, J. (2008). We don't need no architects! *The architecture journal* , 2.

Hoque, F. (2008, June). Is your head in the cloud? *Baseline* , 38-41.

Ingevaldson, P. (2006). IT, We Have A Problem. *Computerworld* , 36.

insecure.org. (2005). *Chapter 15. Nmap Reference Guide*. Retrieved May 15, 2008, from insecure.org: http://nmap.org/book/man.html

Insecure.org. (2006). *Top 100 network security tools*. Retrieved December 2006, from http://sectools.org/

Institute of Directors. (2002). *Executive Summary of King Report 2002.* Parktown: South African Institute of Directors.

Intellitactics. (2007). Intellitactics SAM. Reston, Virginia, USA.

ISO. (2006). *ISO/IEC 17799:2005 Information Technology - Security Techniques - code of practice for information security management*. Retrieved February 2007, from http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

ITGI. (2000, July). CobiT 3rd Edition framework.

ITGI. (2007). CobiT 4.1 Executive summary. USA.

ITGI. (2007). CobIT Security Baseline version 2 - An Information Security Survival Kit. United States of America.

ITGI. (n.d.). *Information Security Governance - Top Actions for Security Managers.* Retrieved August 15, 2007, from IT Governance Institute.

ITGI. (2005). *IT Alignment: Who is in charge?* Rolling Meadows.

Karygiannis, T. (2008). Five Questions with Tom Karygiannis. *Information systems control journal , 2*, 18-19.

Kim, S., Kim, S., & Lee, G. (2006). Structure design and test of enterprise security management system with advanced internal security. *Future Generation Computer Systems* , 1-6.

Kimball, R., & Ross, M. (2002). *The data warehouse toolkit: the complete guide to dimensional modeling* (2nd Edition ed.). USA: Wiley Computer Publishing.

KM World. (2007, January). Enforcing security for EOUSA. *KM world* , 6.

Leo, M. (2008). End Point Security. *Information System Control Journal , 2*, 33-35.

Macaulay, A. (2004, January). Enterprise Architecture design and the integrated architecture framework. *Microsoft Architects Journal* , 4-9.

Mallin, C. (2006). *Handbook on international corporate governance.* Cornwall, UK: MPG Books Ltd.

Marakas, G. M. (2003). *Decision Support Systems in the 21st century* (2 ed.). Upper Saddle River, New Jersey, USA: Pearson Education, Inc.

Marakas, G. M. (2003). *Modern Data warehousing, mining, and visualization core concepts.* Upper Saddle River, New Jersey, USA: Prentice Hall.

Marchewka, J. T. (2003). *Information Technology project management. Providing measurable organizational value.* USA: John Wiley & Sons.

Mccormick, J. (2007, May). 6 Keys to SOA success. *Baseline* , 12.

McLaughlin, M. (2008, May). All in the game. *Best's Review* , p. 100.

McLeod, R. (1983). *Management Information Systems* (2nd Edition ed.). USA: Science Research Association.

McRee, R. (2007). Security Officer Management & Analysis Project (SOMAP). *ISSA journal* , 32-34.

Messmer, E. (2005). Security mgmt. advances. *Network world* , 12.

Mitropoulos, S., Patsos, D., & Doulgigeris, C. (2007). Incident response requirements for distributed security infomration management systems. *Information management & computer security , 15* (3), 226-240.

Moulton, R., & Coles, R. (2003). Applying Information Security Governance. *Computers and Security* , 580-584.

Naidoo, R. (2002). *Corporate Governance an Essential Guide for South African Companies.* Cape Town, South Africa: double Storey Books.

netForensics. (2007). netForensics nFX SIM One. Edison, NJ, USA.

netForensics. (2007). *nFX SIM One*. Retrieved May 23, 2008, from netForensics: http://www.netforensics.com/products/Sim_One/

Netstumbler.com. (2007). *About Netstumbler.com*. Retrieved May 15, 2008, from Netstumbler.com: http://www.netstumbler.com/about/

Nohlberg, M., & Backstrom, J. (2007). User-centred security applied to the development of a management information system. *Information management and computer security , 15* (5), 372-381.

O'Brien, J. A. (1999). *Management Information Systems: managing information technology in the internetworked enterprose.* USA: Irwin/McGraw-Hill.

OECD. (2005). *OECD Principles of Corporate Governance.* OECD.

Olivier, C. (2006). *MoVIS: A Model for the visualization of information security.*

Olivier, M. S. (1997). *Information Technology research - a practical guide.* Johannesburg, South Africa.

O'Reilly, A. (2006, September/October). Continuous auditing: Wave of the future? *The corporate board* , 24-26.

Peterson, R. (2004). Crafting Information Technology Governance. *Information systems Management* , 7 - 22.

Pfaffenberger, B. (1997). *Dictionary of computer terms* (6th Edition ed.). New York, USA: Simon & Schutster, Inc.

Pipkin, D. L. (2000). *Information security - protecting the global enterprise.* Upper Saddle River, New Jersey: Prentice Hall PTR.

Pironti, J. P. (2007). Developin metrics for effective information security governance. *Information Systems Control Journal , 2*, 36.

Platt, M. (2002, July). *MSDN*. Retrieved October 21, 2008, from Microsoft Architecture overview: http://msdn.microsoft.com/en-za/library/ms978007(en-us,printer).aspx

PlexObject Solutions. (2006). *PlexCrypt - Cryptography Toolkit*. Retrieved May 20, 2008, from PlexObject Solutions: http://www.plexobject.com/software/plexcrypt/index.html

Raghuphati, W. (2007). Corporate Governance of IT: A Famework for Development. *Communications of the ACM* , 94-99.

Rapid 7. (2008). *NeXpose*. Retrieved May 20, 2008, from Rapid7.com: http://www.rapid7.com/vulnerability-assessment.jsp

Rich, A. (2005, October). *Feature Article - Analyzing Snort data with the Basic Analysis and Security Engine (BASE).* Retrieved May 19, 2008, from BigAdmin System Administration Portal: http://www.sun.com/bigadmin/features/articles/snort_base.html

Robertson, B., & Raddeman, B. (2004). Thinking beyond the traditional receivables asser behaviour dashboard. *Healthcare financial maangement* , 80.

Robinson, B. (n.d.). *Security dashboards - Are high-level views the answer to getting managers the cybersecurity status information they need to make decisions?* Retrieved May 2006, from 2005: http://www.fcw.com/article91327-11-07-05-Print#related

Ross, S. J. (2008). Reliable security. *Information System Control Journal , 5*, 9-10.

Rozanski, N., & Woods, E. (2005). *Software systems architecture: working with stakeholders using viewpoints and perspectives.* Upper Saddle River, New Jersey, USA: Pearson Education, Inc.

Sambamurthy, V., & Zmud, R. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. *MIS Quaterly* , 261-290.

Sandrino-Arndt, B. (2008). People, portfolios and processes: The 3P model of IT governance. *Information System control journal , 2*, 36-39.

Sardoni, K. (2002, October 7). Executive dashboards - a vision of the business enterprise. *The enterprise* , pp. 16-17.

Savant Protection. (2007). *Savant Enterprise Management System*. Retrieved May 20, 2008, from Savant protection: http://www.savantprotection.com/sems.htm

SC Magazine. (2008). *SC Magazine Awards*. Retrieved May 20, 2008, from SC Magazine: http://www.scmagazineuk.com/Awards/section/341/

SC Staff. (2008, April 23). *SC Awards europe 2008: Winners announced*. Retrieved May 19, 2008, from SC Magazine: http://www.scmagazine.com/uk/news/article/804222/sc-awards-europe-2008-winners-announced/

Searcy, D. L., & Woodroof, J. B. (2003, May). Continuous auditing: leveraging technology. (R. H. Colson, Ed.) *The CPA journal* , 46-48.

Sebor, J. (2008, May). Seven steps to SOA success. *CRM magazine* , pp. 33-37.

Secure Computing corporation. (2008). *Secure Firewall*. Retrieved May 20, 2008, from Secure computing: http://www.securecomputing.com/index.cfm?skey=20&lang=en

Shipley, G. (2006, May 22). *Market Analysis: Security Information Management.* Retrieved May 19, 2008, from Network Computing: http://www.networkcomputing.com/channels/security/showArticle.jhtml?queryText=&articleID=187203568&pgno=1

Shipley, G. (2002, April 1). Security Inforamtion management tools: Netforensics leads a weary fleet. *Network Computing* , pp. 51-59.

Smith, F. (2008, June). As SOA adoption solidifies, good governance is recognized as critical next step. *Manafacturing Business Technology* , 48-49.

Snort.org. (2008, May 13). *SNORT.ORG*. Retrieved May 19, 2008, from SNORT.ORG: http://www.snort.org/

SOMAP.org. (2007). *SOBF - Information security governance, risk and compliance tool*. Retrieved May 20, 2008, from SOMAP.org: http://www.somap.org/sobf/

SOMAP.org. (2007). *What is SOMAP.org?* Retrieved May 20, 2008, from Security Officers Management & analysis Project: http://www.somap.org/default.html

SourceFire. (2008). *The SourceFire 3D System*. Retrieved May 20, 2008, from SourceFire: http://www.sourcefire.com/products/3D/

Sperley, E. (1999). *Enterprise data warehouse: planning, building, and implementation.* Upper Saddle River, New Jersey, USA: Prentice Hall PTR.

Sprott, D. (2005). *CBDI Report. Bussiness flexibility through SOA.* CBDI Forum Limited.

Stephenson, P. (2006, September). Trigeo SIM. *SC Magazine* , p. 16.

StillSecure. (2008). *Safe Access*. Retrieved May 20, 2008, from StillSecure: http://www.stillsecure.com/safeaccess/index.php

Sveen, F. O., Sarriegi, J. M., Rich, E., & Gonzalez, J. J. (2007). Toward viable information security reporting systems. *Informaiton management & computer security* , *15* (5), 408-419.

Swanson, M., & Guttman, B. (1996, september). Generaly accepted pronciples and practices for security information technology systems. *NIST 800-14* .

Taft, D. K. (2008, May 19). Improving SOA security. *eWeek* , p. 26.

Technology Pathways. (2008). *ProDiscover computer forensics home*. Retrieved May 20, 2008, from techpathways.com: http://www.techpathways.com/DesktopDefault.aspx

Tenable network security. (2008, April 4). *pr91*. Retrieved May 19, 2008, from Tenable network security: http://www.nessus.org/news/data/pr91.pdf

Tenable Network security. (2008). *Tenable Network security news*. Retrieved May 15, 2008, from Tenable Network Security: http://www.tenablesecurity.com/news/

The Snort Project. (2008, March 12). Snort Users Manual 2.8.1.

Thiagarajan, V. (2006, May 3). SANS audit check list.

Top Layer Security. (2008). *Intrusion Prevention System Products*. Retrieved May 20, 2008, from Top Layer: http://www.toplayer.com/content/products/intrusion_detection/attack_mitigator.jsp

Trend Micro. (2008). *Interscan Gateway Security Appliance*. Retrieved May 20, 2008, from Trend micro: http://us.trendmicro.com/us/products/mb/interscan-gateway-security-appliance/

TriGeo Network Security. (2007). Taking Networks security to a whole new level.

Trigeo. (2007). *Trigeo Security Information Mangement*. Retrieved May 20, 2008, from Trigeo: http://www.trigeo.com/products/

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, Processes and Relational Mechanisms for IT governance. In W. Van Grembergen, *Strategies for Information Technology Governance* (pp. 1-36). USA: Idea Group Publishing.

Von Solms, B. (2001). Information security - A multidimensional discipline. *Computers and security , 20* (6), 504-508.

Von Solms, B. (2006). Information Security - The Fourth Wave. *Computers and Security* , 165-168.

Von Solms, B. (2005). Information Security Governance: CobIT or ISO 17799 or both? *Computers and Security* , 99 -104.

Von Solms, R., & Von Solms, B. (2006). Information Security Governance: A Model Based on The Direct-Control Cycle. *Computers and Security* , 408-412.

W3C. (2004, February 11). *Web services glossary*. Retrieved July 24, 2008, from W3C: http://www.w3.org/TR/ws-gloss/

Ward-Dutton, N., & Macehiter, N. (2005, November). *Application delivery and SOA: a lifecycle approach.* Retrieved July 22, 2008, from www.mwdadvisors.com.

Weill, P. a. (2004). *IT Governance. How Top Performers Manage IT Decision Rights for Superior Results.* Boston, Massachusetts: Harvard Business School Press.

Wetstone Technologies. (2008). *LiveWire Investigator*. Retrieved May 20, 2008, from Wetstonetech.com: https://www.wetstonetech.com/cgi/shop.cgi?view,14

Whitman, M. E., & Mattord, H. J. (2004). *Management of information security.* Canada: Thomson Course Technology.

Whitman, M. E., & Mattord, H. J. (2004). *Management of information security*. Canada: Thomson course technology.

Williams, P. (2007, August). Executive and board roles in information security. *Network Security* , 11-14.

WinterGreen Research. (2008). Services Oriented Architecture (SOA) Infrastructure Market Shares, Market Strategy, and Market Forecasts, 2008-2014. Lexington, Massachusetts, USA: Wintergreen research, inc.

Wixley, T., & Everingham, G. (2005). *Corporate Governance second edition.* Cape Town, South Africa: Siber Ink CC.

Wood, C. C. (1996). Information owners, custodians and users. *Inforamtion management & computer security* , 34-35.