INFORMATION SECURITY: A CORPORATE GOVERNANCE ISSUE

E. Kritzinger - von Solms, L.A.M. Strous
Department Computer Science and Information Systems, University of South Africa, Pretoria, South Africa, e-mail: ***kritze@unisa.ac.za****,*
Payment Systems Policy Department, De Nederlandsche Bank NV, Amsterdam, The Netherlands, e-mail: ***strous@iaehv.nl***

Abstract: Information is a valuable resource for any organisation today and is critical for the success of the organisation. It is the corporate board's responsibility to ensure the success of the organisation; therefore the board is also responsible for the information security in the organisation. This paper addresses the questions whether the current reference documents on corporate governance pay sufficient attention to information security and whether reference documents on security management and baseline controls sufficiently recognise the relationship with internal control systems and governance framework and specifically pay attention to the responsibilities of the corporate board with respect to information security.

Key words: information security management, internal control, corporate governance, IT governance

1. INTRODUCTION

"Corporate governance is the system by which companies are directed and controlled." Cadbury Report [7]

In an increasingly competitive world, the company with the best information on which to base management decisions is the most likely to win and prosper [1]. Organisations must understand that information is a very valuable resource that must be protected and managed accordingly.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35693-8_16
M. Gertz (ed.), *Integrity and Internal Control in Information Systems V*

According to the International Federation of Accountants [2] information security relates to the protection of information against loss, disclosure or damage. The purpose of information security is to ensure business continuity and reduce business damage by preventing and minimising the impact of security incidents. Security incidents ranging from hacking attempts to viruses (like Melissa) cost businesses around the globe more than $1.5 trillion in 2000 [3].

Until early 1990, it was the responsibility of one specific person or department to maintain information security in the organisation. The majority of the employees, however, did have little knowledge of information security issues in the organisation. The attitude among employees was usually that if something went wrong in information security, it was the information technology department's fault.

This attitude started to change over time. The responsibility of information security shifted from one person (or department) to the entire organisation. Employees are being forced to understand and implement information security on a day-to-day basis. This responsibility of information security is being implemented at senior management level as well as at the level of all other employees in the organisation. The reason for implementing information security at the top level is that when senior management personnel take responsibility for it, the rest of the organisation will follow.

According to Nicholas Durlacher, the Securities and Futures Authority (SFA) chairman [4], senior executives do not have to take responsibility for all the actions of their employees. However, organisations have the right to require senior executives formally to justify their conduct and competence in the event of a management failure, which is so serious that it threatens the future of the firm.

Yet, not all companies are taking security issues as seriously as they should. A December 1999 survey by US-based research house ICD found that one out of five large companies - those with over 1000 employees - did not have efficient information security procedures. That means that information security is not taken seriously on higher levels.

The role of information security in Corporate Governance is not a new issue. In 1996 Ken Lindup stated senior management have never been so dependent on information security as they are today. All the signs are that this dependency can only increase [4]. Therefore it is essential that corporate

management include information security as a vital part of governing an organisation. The questions that can be asked are: "Do corporate governance documents actually address information security and if so, to what extent?" and "Do information security documents sufficiently recognise the responsibilities of the board? "

Chapter 2 will explain the relationship between corporate governance, internal control and information security. Chapter 3 contains an introduction to the documents on corporate governance and information security that can be found in the business environment across the globe. Chapter 4 will discuss some observations and conclusions concerning the coverage of information security responsibilities in corporate governance documents and of governance aspects in information security management guidelines.

2. INFORMATION SECURITY: A CORPORATE GOVERNANCE ISSUE - ROLES, TASKS, RESPONSIBILITIES

2.1 Definitions

2.1.1 Corporate governance

According to the Peters' report [5], the King report [6] and the Cadbury report [7] a definition for corporate governance is:

- Governance is about administration and management, about responsibility and control, and about disclosure and supervision.
- The concept of corporate governance is understood to mean a code of conduct for those associated with the company - in particular directors, Supervisory Board members and investors - consisting of a set of rules for sound management and proper supervision and for a division of duties and responsibilities and powers effecting the satisfactory balance of influence of all the stakeholders. The basic principle here is that members of the Board of Directors and Supervisory Board members should - also in public - be accountable for their conduct.
- The board's actions are subject to laws, regulations and shareholders in general meeting.

2.1.2 Internal control

A widely accepted definition of an internal control system (ICS) is the following [8, 9, 10]

"An ICS can be regarded as the process, including all the controls, financial or otherwise, effected by the board of directors, senior management and other personnel to provide reasonable assurance that the following objectives are achieved:

a. accomplishment of established goals and objectives;
b. economical and efficient use of resources;
c. adequate control of the various risks incurred and the safeguarding of assets;
d. reliability and integrity of financial and management information;
e. compliance with laws and regulations as well as policies, plans, internal rules and procedures."

Internal control can help an entity achieve its performance and profitability targets, and prevent loss of resources. It can also help to ensure that the enterprise complies with laws and regulation avoiding damage to its reputation and other consequences [10]. The Governing Board must take the overall responsibility for ensuring the establishment and maintenance of a sound system of internal controls.

2.1.3 Information Security (Management)

There are many definitions of information security and information security management. In this paper we have chosen the terminology of the ISO GMITS technical report [11]:

IT security is defined as: all aspects related to defining, achieving and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability.

A systematic approach is necessary for the identification of requirements for IT security within an organisation. This is also true for the implementation of IT security and its ongoing administration. This process is referred to as the management of IT security.

2.2 Role & responsibility of the board

The board is ultimately responsible for the organisation's success, and is therefore responsible for the protection of information in the organisation.

The board can also be held accountable for loss, damage or theft of information in the organisation. That means information security must be formally addressed in the corporate governance documents of the organisation to be successful.

The board is therefore responsible for the confidentiality, integrity and the availability of information. To make sure these three aspects of information security are enforced, the organisation can make use of internal controls that includes guidelines and baseline controls. The relationship between corporate governance, internal control, and information security can be depicted in the figure below.

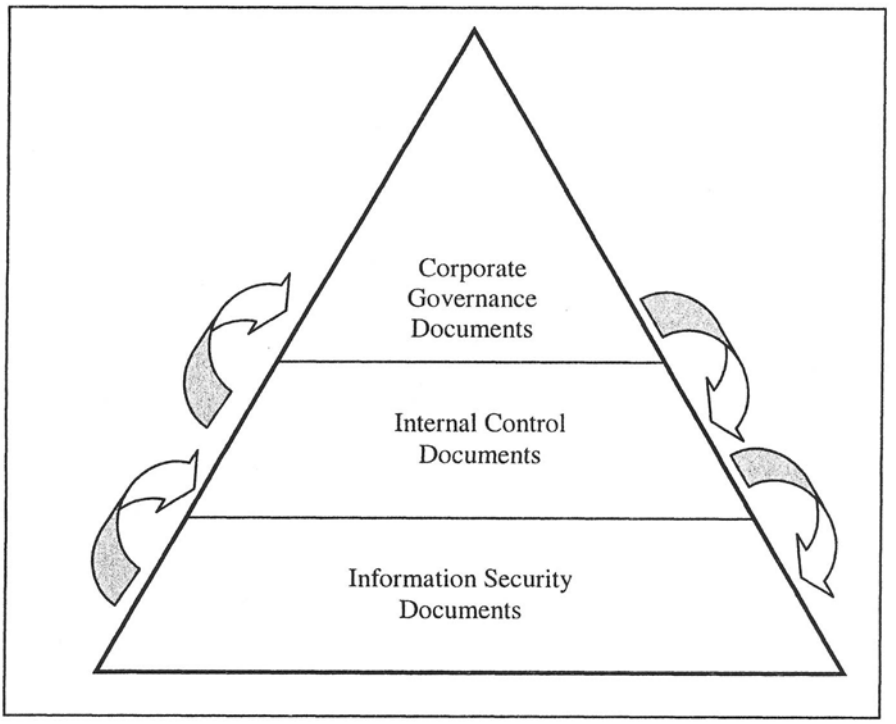

Figure 1: Relationships between corporate governance, internal control, information security

The responsibilities of the board towards information security must be structured in such a way that it forms part of the corporate governance documents, internal control documents and also fit into the overall structure of information security management in the organisation.

IT governance usually occurs at different layers, with team leaders reporting to and receiving directions from their managers, with managers reporting up to executive, and the executive to the board of directors [12].

The figure below depicts a possible example of the structure of the roles and reporting lines with respect to information security in an organisation.

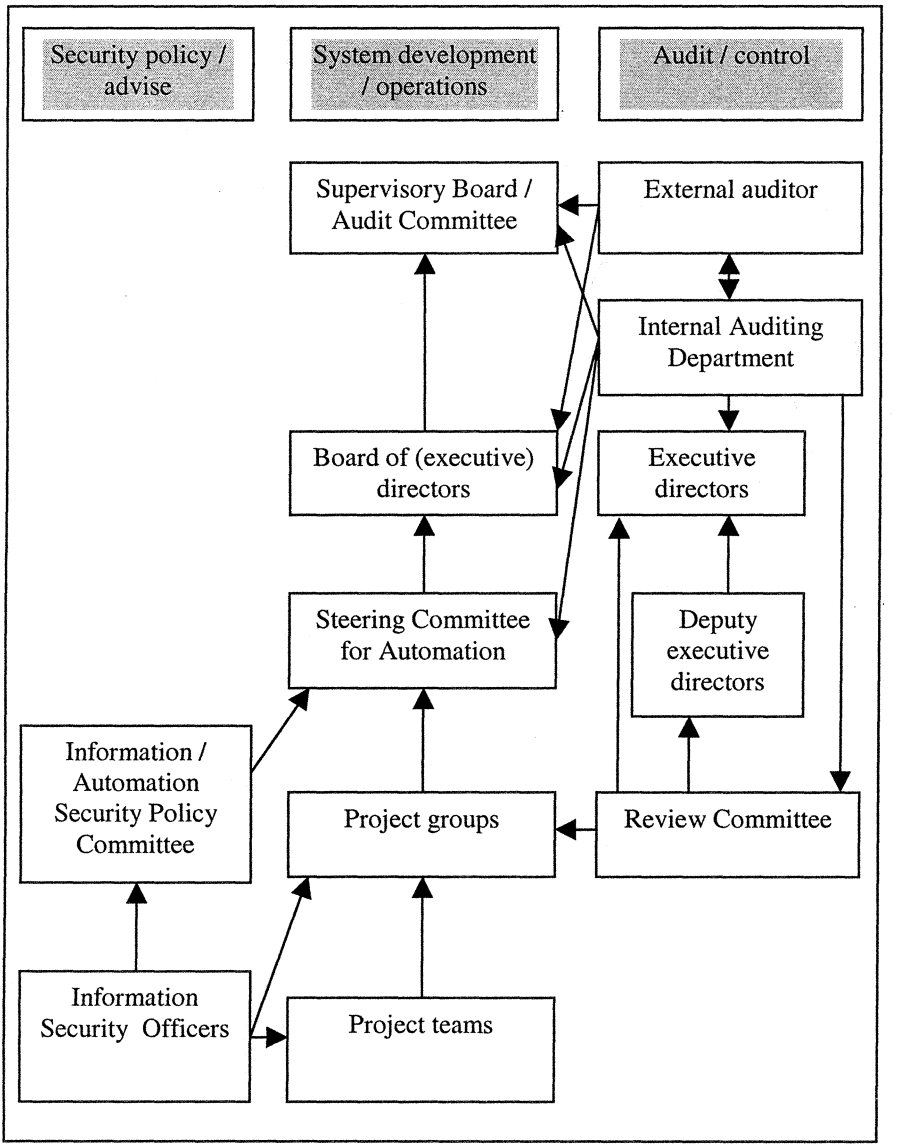

Figure 2: Roles in information security and reporting lines.

It is up to the board to obtain the orientation and training required to understand and govern information security successfully in the organisation. The board is also responsible to ensure that all stakeholders (such as employees) are aware of all information security rules and regulations

through information security training. The reason for this is that before information can be properly secured and managed the board, management and stakeholder must recognise the overall importance of information security and the governance thereof.

One reason why it is very difficult to govern information security is because of the rapid growth of information security technology around the globe. It is the responsibility of the board to ensure that the correct internal control and information security documents are in place to address these issues. The board should encourage effective and responsible use of information technology. The organisation should have a strategy to exploit available technology without endangering itself or its neighbours [13]. It is thus the board's responsibility to ensure that the organisation' internal controls are up-to-date with the newest developments of information security.

Therefore internal controls are the responsibility of the board and information security issues must be included in the internal controls. In the next section of this paper different documents on corporate governance, security management, and baseline controls will be mentioned and investigated in detail.

3. DOCUMENTS ON (CORPORATE) GOVERNANCE, INTERNAL CONTROL AND INFORMATION SECURITY

This chapter contains an introduction to the current documents on the topics in the title. These documents are examined for their coverage of governance and security issues (as meant in the abstract).

3.1 Documents on internal control and (corporate) governance.

3.1.1 COSO Internal Control - Integrated Framework

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) was formed to redefine internal control and the criteria for determining the effectiveness of an internal control system in an organisation. In 1992 a document was published: *Internal control - Integrated Framework* [10]. This document has become a standard reference

work with respect to the topic of internal control systems and it is often referred to as "the COSO report" or just "COSO". Since it has had such an impact, it is interesting to quote the definition of internal control:

"Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations;
- Reliability of financial reporting;
- Compliance with applicable laws and regulations. "

The COSO report deals with internal control from a viewpoint of five interrelated components:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring.

During the ten years since the publication of the COSO framework, many other reports have been written on internal control systems. These reports have expanded on the COSO framework or have taken a slightly different angle, but still all of them have their foundation in the COSO report.

In the COSO report, a few pages are dealing with control over information processing and information systems. No explicit reference is made to (corporate) governance frameworks, although roles of the board of directors and special committees are described.

3.1.2 Guidance on Control

This is the first publication [14] in a series on Control and Governance, published by the Canadian Institute of Chartered Accountants (CICA, 1995). The guidance offers a framework for making judgements about control. It gives a definition of control and twenty "criteria of control" are described and discussed. The document refers to the COSO Internal Control - Integrated Framework [10] but does not deal with information security nor with (corporate) governance.

3.1.3 Guidance for Directors - Governance Processes for Control

This very brief document [15] is the second publication in the series on Control and Governance, by the Canadian Institute of Chartered Accountants (CICA, 1995) and it provides guidance for a board of directors to fulfil its responsibility for control, as part of the governance processes in an enterprise. Information security (management) is not specifically mentioned.

3.1.4 Internal Control Systems of Credit Institutions

Issued by the Banking Supervisory Sub-Committee of the European Monetary Institute (EMI) in 1997, this report [8] contains general considerations on internal control systems of credit institutions from a supervisory perspective. It is based on the COSO report [10] and on work done by several other organisations like the Institute of Internal Auditors (IIA). Information security is addressed in a number of principles relating to information systems and principles relating to electronic information systems, however not in a structured information security management approach.

3.1.5 OECD – Principles of Corporate Governance

In 1999 the Organisation for Economic Co-operation and Development (OECD) published principles [17] that were created to aid government and non-government members to evaluate and improve the framework of corporate governance in their countries. This document shows the importance of corporate governance issues aimed at publicly traded companies across the globe. The document consists of two parts where the first part covers issues ranging from the responsibilities of the board to the rights of the stakeholders.

These principles are mainly derived from governance concepts currently in literature and are presented in five areas:

- the rights of shareholders;
- the equitable treatment of shareholders;
- the role of shareholders;
- disclosure and transparency;
- the responsibilities of the board.

3.1.6 CobiT - Governance, Control and Audit for Information and Related Technology

This comprehensive work [18] is actually a "family of products" and it is an international and generally accepted IT control framework enabling organisations to implement an IT governance structure throughout the enterprise. First published in 1996 by the Information Systems Audit and Control Foundation (ISACF), the third edition was published by the IT Governance Institute (which was founded in 1998 by the ISACF and ISACA, the Information Systems Audit and Control Association). The "family of products" includes an executive summary, the framework, management guidelines, detailed control objectives, audit guidelines and is completed by an implementation tool set.

The main objective of the COBIT project is the development of clear policies and good practices for security and control in IT. The control objectives are primarily developed from the business objectives and needs perspective. COBIT bridges the gaps between business risks, control needs and technical issues and for that purpose it has expanded on existing work in business control models (like COSO) and IT control models (like the Security Code of Conduct of the UK Department of Trade and Industry). COBIT distinguished three types of requirements with respect to information:

- Quality requirements (quality, cost, delivery);
- Fiduciary requirements (effectiveness and efficiency of operations, reliability of information, compliance with laws and regulations);
- Security requirements (confidentiality, integrity, availability).

Furthermore, within the framework, COBIT distinguishes IT processes in four domains:

- Planning and organisation;
- Acquisition and implementation;
- Delivery and support;
- Monitoring.

Within these domains, control objectives are defined for the processes according to the following approach: "The control of IT Processes which satisfy Business Requirements is enabled by Control Statements considering Control Practices."

The framework does not explicitly deal with information security management.

3.1.7 King Report – The code of corporate practices and conduct

The King Report [6] is issued by the Institute of Directors and is a comprehensive document that recommends a Code of Corporate Governance and Conduct for companies in South Africa. The 2001 release of the King Report is a review of the 1994 version and includes new aspects that have an influence on the private as well as the public sector. These additions to the King Report are because of international circumstances and ongoing development in South Africa. The King Report consists of six sections that cover relevant aspects to promote the highest standard of corporate governance.

3.1.8 Board briefing on IT Governance

This recent publication [12] is aimed to be an educational resource for boards of directors, executive management and information technology control professionals. The publication is based on the Control Objectives for Information and Related Technology (COBIT), 3rd edition, an open standard by the IT Governance Institute, the Information Systems Audit and Control Foundation (ISACF) and the Information Systems Audit and Control Association (ISACA).

In this publication, enterprise governance is defined as "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise´s resources are used responsibly." Given the increasing dependency on IT, a special focus on IT governance is advocated. It is stated that "IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives." In this publication, information security is only briefly addressed as one of the objectives to be met: "for IT-related risks to be managed appropriately." Publication [19] deals more extensively with information security.

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

With the same aim and background as [12], this publication deals with questions like "What is information security", "Who should be concerned

with information security governance", "What should the Board and Management do", etcetera. The interesting and important issue in this document is the relationship between information security, IT governance and enterprise (or corporate) governance. One of the tasks of the Board and Executive Management is to ensure that information security fits in the IT governance framework because "effective security is not just a technology problem, it is a business issue. ..... An information security programme is a risk mitigation method like other control and governance actions and should therefore clearly fit into overall enterprise governance." This is one of the very few publications the authors have seen so far where this relationship has been made this explicit.

3.2 Documents on information security (management).

3.2.1 OECD – Guidelines for the security of information systems

The OECD´s guidelines [20] are designed to assist countries and enterprises to construct a framework for security of information systems. Among others, the guidelines are intended to provide a general framework for the development and implementation of effective measures, practices and procedures for the security of information systems. Raising awareness is also an important goal of the publication.

The guidelines identify nine principles with respect to the security of information systems: accountability principle, awareness principle, ethics principle, multidisciplinary principle, proportionality principle, integration principle, timeliness principle, reassessment principle and the democracy principle. Next to the principles, guidance is given for the implementation of security. No reference is made to governance.

Mid 2002 the OECD has published a new version: Guidelines for the security of information systems and networks. This version has not been included in this study.

3.2.2 An introduction to computer security: the NIST Handbook

In the final draft of March 1995, the USA National Institute of Standards and Technology (NIST) states that the purpose of the Handbook [21] is "to provide assistance in securing computer-based resources (including hardware, software and information) by explaining important concepts, cost considerations and interrelationships of security controls." The first section

of the Handbook contains background and overview material, briefly discusses threats and explains the roles and responsibilities of individuals and organisations involved in computer security. The next three sections deal with security controls: Management Controls, Operational Controls and Technical Controls. The Handbook recognises that computer security is an integral element of sound management. No reference is made to governance frameworks.

3.2.3 ISO TR 13569 Information Security Management Guidelines

This is a technical report [22] produced by ISO TC68, the technical committee on Banking, securities and other financial services. The document aims at presenting an information security programme structure and a selection guide to security controls that represent accepted prudent business practice. Also in this technical report (as in ISO PDTR 13335, see 3.2.7) the relationship between different levels of policies is mentioned. And also no reference is made to internal control structures and (corporate) governance frameworks / practices.

3.2.4 ITIL Security Management

As part of the IT Infrastructure Library (ITIL) series of best practice books on different IT services, in 1999 the book on Security Management [23] was published by CCTA (Central Computer and Telecommunications Agency in the UK). The book describes best practices in Security Management and is meant to be of practical assistance and support for IT management. It explains how to organise and maintain the management of security of the IT infrastructure. The book positions security management within the total set of IT processes. It does not position security management within more general internal control structures and governance frameworks.

3.2.5 ISO/IEC 17799: 2000 Code of Practice for Information Security Management

This standard [24] (originally the British Standard BS 7799 which in turn was derived from an industry initiative in 1993 by the same name Code of Practice for Information Security Management) provides a well-proven framework of best practices to implement, maintain and document information security within the organisation. ISO/IEC 17799 defines about 130 security controls structured under 10 headings to enable readers to identify the particular safeguards that are appropriate to their business or specific area of responsibility. These headings are: Security policy, Security

organisation, Asset classification and control, Personnel security, Physical and environmental security, Communications and operations management, Access control, Systems development and maintenance, Business continuity management, Compliance. Although sufficient attention is paid to policy and organisation, no reference is made to governance frameworks.

3.2.6 IT Baseline Protection Manual

The Bundesamt für Sicherheit in der Informationstechnik (BSI, which is the federal German Information Security Agency) has published and maintains an IT Baseline Protection Manual [25] that presents a set of recommended standard security measures or "safeguards" for typical IT systems. The aim of these IT baseline protection recommendations is to achieve a security level for IT systems that is reasonable and adequate to satisfy normal protection requirements and can also serve as the basis for IT systems and applications requiring a high degree of protection. This is achieved through the appropriate application of organisational, personnel, infrastructural and technical standard security safeguards.

The safeguards listed in the IT Baseline Protection Manual are standard security measures, i.e. measures which should be implemented for the modules concerned using the latest available technology in order to achieve a reasonable level of security. In some cases these safeguards also provide a higher level of protection than that required simply to implement a baseline level of protection; nevertheless, they are the minimum security precautions which it is reasonable to implement in the areas concerned.

No reference is made to governance frameworks and internal control systems.

3.2.7 ISO/IEC PDTR 13335-1 GMITS: Guidelines for the Management of IT Security – Part 1: Concepts and models for managing and planning IT security

The GMITS document (ISO/IEC PDTR 13335) is a technical report [11] produced by SC27, the subcommittee on Security Techniques of the ISO/IEC Joint Technical Committee on Information Technology. The technical report is currently under revision according to ISO practices and the studied version is the proposed draft of late 2001. It is a technical report that provides guidance on the management of IT security. The document consists of five parts that address different areas of the management of IT

security. In this paper we concentrate on part 1 (Concepts and models for managing and planning IT security).

In part 1 concepts and models are presented that are considered to be basic for an understanding of IT security. It addresses the general management issues concerning the planning, implementation and operation of IT security. Besides a nice introduction to IT security organisation and security management functions, a strong point in this document is the fact that a hierarchy of policies is given in which the IT security policy is incorporated. This emphasises the fact that an IT security policy should be derived from a corporate business policy and a corporate security policy, and should take into account issues from other policies like for instance the corporate IT policy.

No reference is made to internal control structures and (corporate) governance frameworks / practices.

3.2.8 Draft BS 7799-2: 2002 Information Security Management Systems - specification with guidance for use

As an addition to BS 7799-1 Code of Practice for Information Security Management, this part [26] has been developed to provide a model for establishing, implementing, maintaining and improving an effective Information Security Management System (ISMS). Such an ISMS must ensure adequate and proportionate security controls to protect information assets. The control objectives and controls in this part are derived from ISO/IEC 17799: 2000.

Reference is made to quality management systems for instance, but not to governance frameworks.

4. OBSERVATIONS AND CONCLUSION

4.1 Observations

The brief literature study has shown that, with the exception of the two recent IT Governance Institute publications [12] and [19], the internal control and (corporate) governance documents do not address information security (management) extensively and/or explicitly. Although these documents deal to a great extent with the responsibilities of the board of

directors and senior management, specifically mentioning that information security is one of these responsibilities is seldom seen.

One reason why information security is not yet included in management level documents may be that there is no need or pressure for industry to include them in the documents. Only when industry develops a specific need or realizes the importance of information security, they will be included in the management documents. This however takes time and usually only appears in the revised versions of the documents. The industry needs are frequently demand driven, due to for example new technologies, or effect driven such as the ENRON (and other) corporate scandals.

Another reason may be the fact that the members of boards of directors have a direct (personal) interest in many other corporate governance aspects, such as procedures on appointments, remunerations, reporting and on personal investments in the company. Information security is of a different nature for them, less personal and therefore not in the focus of their attention.

Also due to the misconception that information security is a purely technical issue, it is not getting the attention it should get in risk management processes and that is another possible reason for not being included in many documents. As an opposite to this, sometimes documents such as the King Report do not address information security on its own but they add it under the main heading Risk Management. If the reader is not aware of this, they will think that information security is not addressed at all.

As far as the information security documents are concerned, no clear references or explanation of relationships to internal control systems or (corporate) governance frameworks could be found.

One explanation for this is that information security is still very often seen as a technical aspect that must be addressed on a technical level. It is essential that industry first adopts information security as a management issue before references to internal control and corporate governance frameworks will be seen.

Another reason for this is the fact that different types of specialists are dealing with information security and with internal control and governance. Information security is usually dealt with, also in standardization activities, by technical experts who do not often have a background in or knowledge of control and governance. On the opposite, experts in the areas of control and governance do not know a lot about technical security aspects. This indicates

that there is a need for co-operation between the different disciplines and that curriculae and training programmes should pay attention to this.

The authors believe that this situation will change due to the increasing pressure from business partners and shareholders to ensure the sound management of information security in the entire organization. This can only be done if information security is addressed on a (corporate) governance level. The reason for this is that if senior management takes responsibility for information security, the rest of the organization will follow.

4.2 Conclusion

There is no doubt that information is vital for the success of any organisation. Information must therefore be protected against all kinds of threats, whether by man or nature, whether intentional or accidental. This makes information security so important that it must be a responsibility of the board of directors / corporate management. Therefore the corporate management can and must be held accountable for information security management and processes in the organisation. In order to get this message across, it is essential that the main issues from security reference documents / standards are formulated in the "board of directors language".

Since the board of directors nowadays is more used to the (language of) documents on corporate governance, it can be subject for further study in what way governance and security documents can best be combined. We feel that the document "Information Security Governance: Guidance for Boards of Directors and Executive Management" can be a good starting point. This also implies a need for a better understanding of each other and a closer co-operation between the (internal) control specialists and the (information) security specialists. Another argument for this is that the internal and external auditors (control specialists) usually have a more frequent and better entrance to the board of directors than the security specialists.

REFERENCES

[1] *Information systems risk management: Key concepts and business processes,* Thomas Finne, Computers & Security, volume 19 (2000) number 3, pp. 234-242

[2] *Managing Security of Information,* International Federation of Accountants (IFAC), 535 Fifth Street Avenue, Floor 26, New York 10017

[3] *Study Tallies High Expense Of Computer Viruses,* TechWeb News, July 7, 2000, http://content.techweb.com/wire/story/TWB20000707S0004

[4] *The role of information security in corporate governance*, Ken Lindup, Computers & Security, volume 15 (1996) number 2, pp. 477-485

[5] *Corporate governance in The Netherlands - Forty recommendations,* (Peters' report), Committee on Corporate Governance, The Netherlands, June 1997

[6] *The Code of Corporate Practices and Conduct,* (King Report), Institute of Directors, South Africa, version of July 2001

[7] *Report of the Committee on the Financial Aspects of Corporate Governance*, (Cadbury Report), UK, December 1992

[8] *Internal control systems of credit institutions,* Banking Supervisory Sub-Committee of the EMI, July 1997

[9] *Working paper on Internal Control Systems*, prepared by internal auditors of a group of central banks, BIS and EMI, June 1997

[10] *Internal control - integrated framework,* Committee of Sponsoring Organisations of the Treadway Commission (COSO), September 1992

[11] *GMITS: Guidelines for the Management of IT Security, Part 1: Concepts and models for managing and planning IT security,* ISO/IEC JTC1/SC27, PDTR 13335-1 (revision), version 28-11-2001

[12] *Board Briefing on IT Governance*, IT Governance Institute, 2001, ISBN 1-893209-27-X

[13] *A call to action for corporate governance,* developed through the co-operation of the IIA, AICPA, ISACA and NACD, March 2000, http://www.nitc.state.ne.us/tp/workgroups/security/Call_to_action.pdf

[14] *Control and Governance - Number 1: Guidance on Control*, Canadian Institute of Chartered Accountants (CICA), November 1995, ISBN 0-88800-436-1

[15] *Control and Governance - Number 2: Guidance for directors - Governance processes for control* , Canadian Institute of Chartered Accountants (CICA), December 1995, ISBN 0-88800-138-7

[17] *Principles of corporate governance,* Organisation for Economic Co-operation and Development (OECD), 1999

[18] *COBIT – Governance, Control and Audit for Information and Related Technology,* IT Governance Institute / ISACA / ISACF, 3rd edition, 2001, ISBN 1-893209-13-X

[19] *Information security governance: guidance for boards of directors and executive management*, IT Governance Institute, 2001, ISBN 1-893209-28-8

[20] *Guidelines for the security of information systems*, Organisation for Economic Co-operation and Development (OECD), 1992, OCDE/GD(92)190

[21] *An introduction to Computer Security: the NIST Handbook,* National Institute of Standards and Technology (NIST), version March 1995

[22] *Information Security Management Guidelines*, ISO TC68/SC2/ WG4, TR 13569, draft version 30-3-1999

[23] *ITIL Security Management*, Central Computer and Telecommunications Agency (CCTA), 1999, ISBN 0-11-330014-X

[24] *Code of Practice for Information Security Management*, ISO/IEC PDTR 17799: 2000, proposed draft version of November 2001

[25] *IT Baseline Protection Manual*, Bundesamt für Sicherheit in der Informationstechnik (BSI), version 2001

[26] *Information security management systems - specification with guidance for use,* British Standards Institute (BSI), final draft BS7799-2: 2002