IST-Africa 2008 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2008
ISBN: 978-1-905824-07-6

Building a World Class Information Security Governance model

Marthie LESSING[1], SH VON SOLMS
[1]*CSIR, PO Box 395, Pretoria, 0001, South Africa*
Tel: +27 12 8412838, Fax: + 27 12 8414750, Email: marthie.lessing@gmail.com
[2]*University of Johannesburg, PO Box 524, Aucklandpark Kingsway Campus, Johannesburg, 2006, South Africa*
Tel: +27 11 5592843, Fax: + 27 11 5592138, Email: basievs@uj.ac.sa

Abstract: The lack of a fully inclusive guideline document to assist the functioning of sufficient Information Security Governance is common in the business environment. This article focuses on developing such a guideline document, based on a number of best practice documents. The resulting model covers all the relevant aspects on strategic, management and technical level when implemented altogether. This model includes the related aspects of Corporate Governance, Information Technology Governance and Information Security Governance. By applying a best practice driven Information Security Governance model, an organisation ensures that all aspects regarding Information Security Governance are covered in detail. Additionally, the implementation of the best practice driven Information Security Governance model allows organisations to conform to major best practice documents, standards and legal documents.

Keywords: Information Security, Information Security Governance, Corporate Governance, Information Technology Governance, best practice documents, King II Report, Organisation for Economic Co-operation and Development, Sarbanes-Oxley Act, Control Objectives for Information and related Technologies, Information Technology Infrastructure Library, ISO 17799, Standard of Good Practice for Information Security

1. Introduction

"As a general rule the most successful man in life is the man who has the best information." These words from Benjamin Disraeli illustrates why it is in the best interest of modern organisations to govern all aspects of information properly. It is necessary to secure the information in such a way that it can truly contribute to the success of an organisation. The generally accepted way to do this is by applying best practices to the information.

The norm is to apply a single best practice document or standard to an organisation. However, there is no sole best practice document or standard that can ultimately be applicable in all situations of every organisation [1]. Therefore, it is suggested that a model is developed that combines all the best features of a number of best practices and standards. In this way it is possible to build a world class Information Security Governance model from which applicable practices can be selected.

1.1 – Motivation for a World Class Information Security Governance Model

Currently organisations can apply any of a number of industry accepted best practices to warrant internal Information Security Governance. However, these documents are often limited in scope and do not consider the contributions of related governance disciplines. Best practice documents such as the ISO 17799 and the Standard of Good Practice for

Information Security capture much information regarding Information Security Governance. Yet, these documents focus more on the Information Security discipline and not the governance aspects. Accordingly, these documents are not inclusive enough to provide a holistic Information Security Governance model. It is therefore necessary to create an inclusive model to consider all possible aspects of Information Security Governance.

The development of a comprehensive model needs to take the best out of a variety of best practice or related Information Security Governance documents. The development process should integrate all core aspects of the different documents to create an exceptional model for Information Security Governance. The relevance of this model would be that its implementation would cover all aspects of Information Security Governance, Information Technology Governance and Corporate Governance. This process will secure information on all possible aspects and dimensions. This model will add a lot of value to the Information Security Governance discipline.

1.2 – The Role of Governance Types in a World Class Information Security Governance Model

Best practice documents guide organisations in establishing a decent governance structure, whilst measuring compliance against the document's guidelines. The implementation of a best practice document ensures that an organisation effectively covers all relevant aspects that can holistically affect the organisation.

There are three primary types of governance relevant to this study: Corporate Governance, Information Technology Governance and Information Security Governance. Corporate Governance is the all-inclusive Governance discipline, relating primarily to the responsibilities of the board of directors and top management. When implemented correctly, Corporate Governance ensures the well being of the entire organisation [2].

Information Technology Governance is a multi-faceted discipline drawing from Corporate Governance. It mainly handles the relationship between Information Technology Management and the business functions of an organisation [3]. Information Security Governance, the most important discipline concerning this study, is a rather complicated discipline. It has recently expanded so much that organisations employ a specific person to handle only Information Security issues [4]. Figure 1 presents the relationship between the disciplines, and positions Information Security Governance within the bigger structure. All three governance types are crucial to a successfully implemented Information Security Governance structure, since all three governance types have some impact on the discipline.

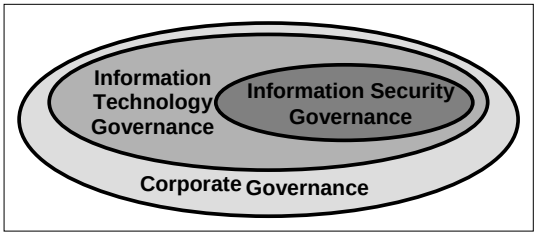

Figure 1: Corporate Governance consisting of a number of disciplines [6]

1.3 – Best Practice Documents as Corner Stone of the Information Security Governance Model

The study focuses on seven best practice documents, standards, guideline documents and legal documents in the various governance disciplines. These documents are all highly regarded and often used by Information Security Governance references studied in the literature review [2]. The documents were chosen as representative of the identified disciplines, balancing the content with regard to all possible key elements. These seven

documents are the King II Report, Sarbanes Oxley (SOX) and OECD from the Corporate Governance discipline, COBIT 3 and ITIL from the Information Technology discipline, and ISO 17799 and the Standard of Good Practice for Information Security from the Information Security Governance discipline.

According to research done in Australia [5], Information Security Governance best practice documents are greatly under utilised and the use of these documents needs promotion worldwide. The thorough implementation of the proposed best practice driven model addresses this problem. The application of such documents can promote organisational competitiveness and innovation. It can assist greatly in the day-to-day running of the organisation on strategic, management and technical level [6].

2. Objectives

Many governance models exist that are applicable to Information Security Governance. Equally, similar models exist for other disciplines related to Information Security Governance [7]. However, there is no model developed solely for Information Security Governance or any model that base on various acknowledged best practice and related documents [8]. Without the implementation of such guidelines, organisations may lack the needed competitive advantage to succeed in the corporate environment.

The objectives of this research is to develop a holistic Information Security Governance model anchored in various available best practices and related documents for Corporate Governance, Information Technology Governance and Information Security Governance. This includes the mapping of the governance disciplines to these best practice documents. The use of this holistic model may ultimately improve the Information Security of the organisation. The reality of this lack of a comprehensive model leads to the problem statement.

3. Methodology

The research methodology is structured to add value to the Information Security Governance discipline by filling an existing void. The study is qualitative in nature and essentially divides into two distinct components: a literature review and the application of the findings from literature in the development of a model for practical implementation.

The majority of the study is a literature research of the selected best practice and related documents regarding Corporate Governance, Information Technology Governance and Information Security Governance. Due to time limitations, this study does not concern the empirical evidence of why organisations in the industry do not commonly implement best practice documents. The study is set on the assumption that organisations are more likely to implement a single, comprehensive model to ensure Information Security Governance and the related governance disciplines, rather than spend time implementing multiple models to ensure full coverage of all the different aspects.

4. Technology Description

Information Security Governance is a key factor in Information Security. It literally means governing the security of information, and is worthless if the organisation does not apply the principles or monitor the compliance. Without Information Security Governance, an organisation has no guarantee of any long-term success. Properly implemented Information Security adds several advantages to an organisation:

- emerging technologies, such as anomaly detection
- the regulatory nature of the discipline
- an increasingly mobile workplace and world [9]

A number of states and regulatory bodies have tried to either create their own Information Security policies [10], or implement existing policies, but none of these implementations was sufficient [11]. None of the individual documents is comprehensive enough regarding the Information Security Governance guidelines. The general outcome was persistent problems regarding implementation and compliance, and a negative attitude towards the discriminatory nature of inconsistent information systems [12]. To counter these problems, the respective documents should combine to produce an inclusive Information Security Governance implementation guide.

5. Developments

The proposed best practice driven model needs to be comprehensive in nature to ensure its adoption into the Information Security industry. Therefore, it is necessary to identify a number of key elements or drivers, as presented by the model's first draft in Figure 2.

Based on in-depth analysis and scrutiny performed, these elements represent the best practice driven Information Security Governance model truly. In the research process, nine drivers were identified from the Corporate Governance best practice and related documents studied, seven drivers from the Information Technology Governance best practice and related documents and fifteen drivers from the Information Security Governance best practice and related documents. Figure 2 shows the 31 identified drivers [13].

Each of the seven Governance based best practice documents, mentioned in Section 1, was also individually analysed and its inclusion in the best practice driven Information Security Governance model scrutinised. The documents each add a number of drivers to the proposed best practice driven Information Security Governance model. Therefore, by combining elements from a variety of documents, the model guarantees the best guidelines from a variety of discipline leaders, and not only the guidelines from one document. A combined document would also cut out the problem for security managers who do not know which document to implement. Information Security Officers need not decide on a single document anymore, since this study presents an effective combination of documents to implement for an ideal Information Security Governance environment.

6. Results

Extracts from each of the seven documents can be put together to form the foundation of the Information Security Governance best practice driven model. By exploring each of these individual drivers, a number of relationships and correlations were discovered between the various drivers.

In order to present a complete best practice driven Information Security Governance model, the 31 drivers are scrutinised exhaustively regarding content, origin and possible implication, to eliminate duplication of drivers. After this process, the research proposes nineteen drivers as the main components of the best practice driven Information Security Governance model, as presented in Figure 3 [13]. Due to the lengthy, technical nature of this elimination process, it is not covered in this article.

This final model for best practice driven Information Security Governance ensures that an implementing organisation covers all aspects of all the different organisational levels. It further ensures that organisations know beforehand what the associated risks are with a specific course of action. Once the model is structured and properly defined, it should be easy for anyone using the model to implement these units of knowledge.

Organisations should address all nineteen identified drivers (refer to Figure 3) to ensure complete Information Security Governance. In the Information Technology society, there is a possibility that a single Information Security incident, caused by a single organisation, can affect the entire society and economy. For that reason, each individual organisation

should ensure its own Information Security and Information Security Governance to fulfil its responsibility as a member of the Information Technology society [15].

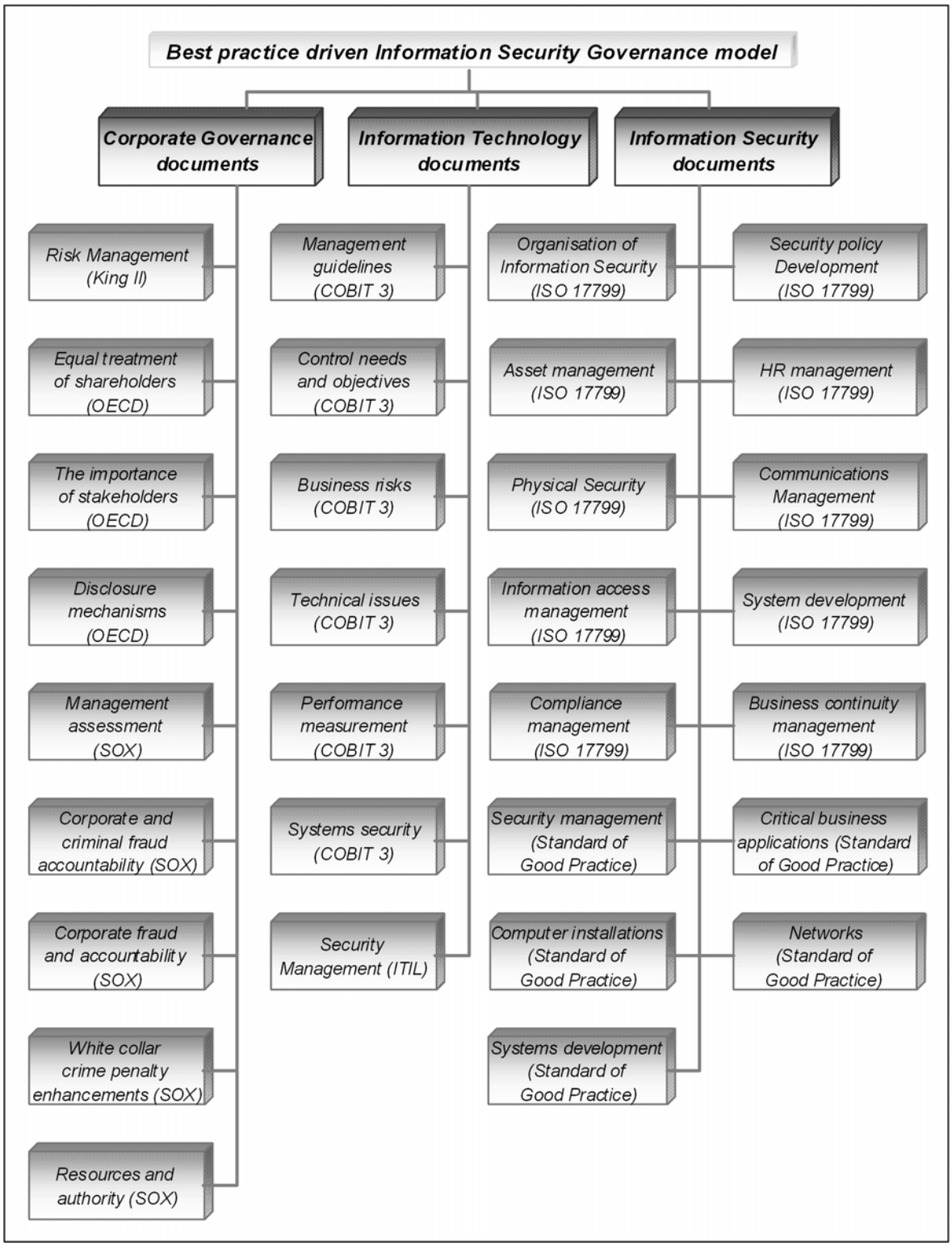

Figure 2: Drivers identified from various governance documents, utilised in the proposed structure for a best practice driven model for Information Security Governance [11]

Some of the best practice documents used as foundation for this study contains most of the nineteen identified drivers. However, the proposed best practice driven Information Security Governance model suggests a more in-depth evaluation of these drivers.

By implementing the best practice driven Information Security Governance model, an organisation is sure to cover more Information Security Governance aspects than allowed with the originally identified informal Information Security Governance model. It can thus be argued that the implementation of single best practice documents is not comprehensive enough to ensure successful Information Security Governance.

Figure 3: Reviewed best practice driven Information Security Governance model [11]

In the majority of aspects considered, the best practice driven Information Security Governance model proved to be more equipped to lead any organisation towards Information Security Governance harmony. With the development of this model, organisations are more likely to implement Information Security Governance successfully. The proposed model is composed of drivers that cover the entire spectrum of Information Security aspects, as identified from the literature review.

7. Business Benefits

Properly implemented Information Security has many advantages. The most prominent advantages are emerging technologies, an increasingly mobile workplace and world, and the regulatory nature of the discipline [12].

From an organisation's point of view, information is an invaluable business tool and thus needs protection just like any other corporate asset. In order to do this an infrastructure is needed to support Information Security, comprising networks, systems and functions that assist in managing and governing information assets [13]. Security application is often a daunting task that requires a huge amount of persistence and perseverance. However, when an organisation overcomes the associated barriers, organisations can focus on reducing the potential for loss, protecting and enhancing business value, and creating competitive advantage [17].

The underlying study [13] has pointed out the dire need for Information Security Governance. Since the risk that a specific Information Security incident will occur is not always obvious, it is difficult for an organisation to invest time and money in Information Security Governance. This Information Security Governance model should therefore be extensive enough to include all possible security scenarios. This should enable any implementing organisation to prevent or indirectly mediate the occurrence of fraud within its perimeters.

Section 2 states that the objective of the research study is to provide an Information Security Governance model of the best practice and related documents. Since this model combines drivers from the Corporate Governance, Information Technology Governance and Information Security Governance disciplines, it can be expected that the Information Security Governance model will inherit a number of the respective best practice and related documents' benefits and advantages, such as uniting the views of customers, employees and suppliers in developing the organisation's strategy [18]. These inherited benefits add enormous value to both the best practice model and the Information Security Governance discipline.

Furthermore, since the purpose of this model is to serve as an aid to both technicians and management involved in the Information Security structure, an implementing organisation can expect to generate the best possible scenario by combining the experiences of a variety of seasoned professionals. Lastly, the convenience of a single document is a very satisfying advantage of implementing the best practice driven Information Security Governance model.

8. Conclusions

This research study addresses the lack of a comprehensive Information Security Governance model based on more than one acknowledged best practice and related documents. In an attempt to solve this problem, the study focused on developing a single model combining all the attributes and advantages of a number of identified best practice related documents.

Since the literature study reveals that the use of a single best practice document in the realisation of Information Security Governance is inadequate, the methodology involved an in-depth inter-disciplinary research analysis to allow for the comprehensive implementation thereof. The aim was to identify a number of key elements from various best practice and related documents that can add value to an Information Security Governance model. These elements were refined and applied on an Information Security Governance platform, to constitute a single holistic model with nineteen elements.

This proposed model is applicable to all organisations, irrespective of size, culture or domain. It combines aspects of Corporate Governance, Information Technology Governance and Information Security Governance to contribute to the successful and secured use of information by any organisation.

Due to the dynamic nature and quick advances in the relevant disciplines, it is necessary to keep a close eye on new developments. By updating the best practice driven Information Security Governance model on a regular basis, the model can remain relevant for many years. The first major revision anticipated for the Information Security Governance model, is to include best practice documents for the Digital Forensic Governance discipline, a relatively new, undiscovered genre. Additionally a detailed comparison may follow between this best practice driven Information Security Governance model, and other recently developed models, such as the model framework presented by the Corporate Governance Task Force [7].

The methodology results in a purely theoretical model of the ultimate implementation of Information Security Governance. For logistical reasons, no organisations are presently implementing the model, but an interactive user guidance document can assist organisations in understanding the model, and accordingly implementing it. Both management and technical level employees can use the model as a checklist of components to address to ensure Information Security Governance in any type of organisation. Alternatively, organisations can map their own security policies on the best practice driven Information Security Governance model to identify security areas that needs more attention.

References

[1] Höne, K. & Eloff, J. H. P. (2002). Information Security Policy - What Do International Information Security Standards Say? *Computers and Security*, 21(5): 402-409.

[2] Von Solms, S. H. & Eloff, H. P. (2004). Information *Security*. Johannesburg: Rand Afrikaans University: 1-93. (Internal document.)

[3] Wikipedia, the free encyclopedia. (2006). Information *Technology Governance.* Available from: http://en.wikipedia.org/ wiki/Information_technology_governance (Accessed on 13 February 2006).

[4] Von Solms, S. H. (2005). Information Security Governance. Compliance management vs operational management. *Computers and Security*, 24(6): 443-447.

[5] Commonwealth of Australia. (2006). *Leading Practices and Guidelines for Enterprise Security Governance.* Trusted Information Sharing Network for Critical Infrastructure Protection. Available from: http://unpan1.un.org /intradoc/groups/public/documents/APCITY/UNPAN024153.pdf (Accessed 6 February 2008).

[6] Cooney, M. C. (2007). *Trusted Information Management: Data Privacy & Security Accountability in Outsourcing*. The Center for Information Policy Leadership. India: Hunton & Williams LLP: 6. Available from: http://www.hunton.com/files/tbl_s47Details/FileUpload265/2054/CIPL_India_White_Paper.pdf (Accessed 6 February 2008).

[7] Cohen, F. (2006). *A Fault Model for Information Security Governance and its Uses as a Basis for Metrics*. Available from: http://all.net/Talks/MiniMetriCon-07.pdf (Accessed 6 February 2008).

[8] Corporate Governance Task Force. (2004). *Information Security Governance - A Call To Action.* Available from: http://www.cyberpartnership.org/InfoSecGov4_04.pdf (Accessed 6 February 2008).

[9] Von Solms, S. H. & Louwrens, C. P. (2006). *The relationship between digital forensics, corporate governance, IT governance & IS governance.* In: *Digital crime and forensic science in cyber space,* edited by P. Kanellis. Washington: Idea Group: 242-265.

[10] Silicon.com. (2007). *Enterprise IT Governance - Senate Review and Study.* Available from**:** http://www.myflorida.com/cio/Presentations/2007/SenateInterimITStudyEnterprise.ppt#256,1 ,Enterprise IT Governance - Senate Review and Study (Accessed on 6 February 2008).

[11] Silicon.com. (2008). *Top Ten Reasons Organisations are Unsuccessful Implementing ITIL*. Available from**:** http://whitepapers.silicon.com/0,39024759,60151250p,00.htm (Accessed on 6 February 2008).

[12] Hancock, B. (2005). *Keynote: The Future of Security: Where are we going?* Paper presented at the Information Security Decision Conference on October 19-21 in New York City. Available from**:** http://infosecurityconference. techtarget.com/html/ci_sessions.htm (Accessed on 20 March 2006).

[13] Lessing, M. M. (2006). *A Model for Best Practice Driven Information Security Governance*. Unpublished dissertation. Johannesburg: University of Johannesburg.

[14] BITS. (2005). *Critical success factors for security awareness and training programs endorsed as voluntary guidelines by the board of Directors of the financial services roundtable*. Washington. Available from: www.bits.com (Accessed on 2 December 2005).

[15] Ishitobi, T. (2005). *Development of Information Security Government.* Ministry of Economy, Trade and Industry. Agenda item: APEC-Business e-Commerce Dialogue - APEC Telecommunications and Information Working Group at Bangkok, Thailand. Document number: Telwg31/ ECOM/05.
[16] Allen, J. (2005*). Governing for Enterprise Security*. Featured in: Networked Systems Survivability Program. Technical Note: CMU/SEI-2005-TN-023. Pittsburgh: Carnegie Mellon University.
[17] *ISO17799 (BS7799) Information Security Standard.* (2006) Available from: http://praxiom.com/iso-17799 2000-outline.htm (Accessed on 6 April 2006).
[18] Minnaar-van Veijeren, M. *The King II report on corporate governance.* Available from: http://www.i-value.co.sa/ king.html (Accessed on 17 November 2005).