INFORMATION SECURITY GOVERNANCE - A RE-DEFINITION

Rahul Rastogi[a] and Rossouw von Solms[b]
[a] *Nelson Mandela Metropolitan University, rahul.rastogi@eil.co.in,*

[b] *Nelson Mandela Metropolitan University, rossouw@petech.ac.za*

Abstract: Information is a fundamental asset of any organization and needs protection. Consequently, Information Security Governance has emerged as a new discipline, requiring the attention of Boards of Directors and Executive Management for effective information security. This paper investigates the literature on Corporate Governance, IT Governance and Information Security Governance to identify the components towards a definition of Information Security Governance. The paper concludes by defining Information Security Governance and discussing the definition, identifying and addressing all important issues that need to be taken into account to properly govern information security in an organization.

Key words: Corporate Governance, IT Governance, Information Security Governance, Information Security

1. INTRODUCTION

Much has been said in recent literature about bringing Information Security into the fold of Corporate Governance, thereby making it a crucial responsibility of the Board of Directors and Executive Management. Information Security Governance has, thus, emerged as a new discipline and responsibility for Board of Directors and Executive Management. But, before Board of Directors and Executive Management can discharge this new responsibility, the term Information Security Governance needs to be defined and understood.

Existing literature provides some guidance on Information Security Governance. However, in the opinion of the authors, this guidance is insufficient. The guidance is prescriptive and does not clearly bring out the meaning of Information Security Governance. In a recent article, the plight of Executive Management with respect to IT Governance is stated as most C-level executives responding to IT Governance with a "frustrated roll of their eyes" (Melnicoff, Shearer & Goyal, 2005, p. 1). We feel that the existing guidance on Information Security Governance will elicit similar reactions.

The objective of this paper is to propose a 'new' definition of Information Security Governance, identifying and addressing all important issues that need to be taken into account to properly govern information security in an organization. The definition answers the following questions:

- What is to be understood from Information Security Governance?
- Who formulates the framework to implement Information Security Governance in an organization?
- Where in the organization is Information Security Governance implemented?
- What are the benefits that Information Security Governance should deliver to the organization?

In proposing the definition of Information Security Governance, this paper first reviews how Information Security is evolving and how it is being brought under the purview of Corporate Governance. It then investigates the existing literature on Corporate Governance, IT Governance and Information Security Governance to identify the components of the proposed definition. The paper concludes by proposing the definition and discussing its various components.

2. THE EVOLUTION OF INFORMATION SECURITY AND THE EMERGENCE OF INFORMATION SECURITY GOVERNANCE

Over the years, IT has penetrated every aspect of modern business and today businesses are critically dependent on IT and information. This has led to the evolution of the role of Information Security. Further, because of the wide impact of information security breaches on organizations, Information Security is increasingly being brought under the fold of Corporate Governance. However, Board of Directors and executive management have very little guidance on what Information Security and Information Security Governance mean for their organization.

Regarding the evolution of Information Security and the emergence of Information Security Governance, two trends emerge from the current literature:

- The role of Information Security is changing – it is no longer about only protecting information assets, but also about assurance and trust (BSA, 2003, p. 3). Information Security is now a competitive weapon.
- Increasingly, Information Security is being linked to Corporate Governance. Many researchers in the field have motivated the need for integrating Corporate Governance and Information Security (von Solms and Thomson, 2003). Further, various regulations and legislation are formalizing this requirement (FISMA, 2002).

Information Security is thus evolving and leading to the emergence of Information Security Governance as a new discipline. Through this evolution and change, Boards of Directors and Executive Management need to understand the value that Information Security delivers for their organization and what they need to do to discharge their responsibility towards Information Security Governance.

This paper attempts to bring the required clarity and understanding by providing a definition of Information Security Governance for Boards of Directors and Executive Management. The following sections investigate the existing literature on Corporate Governance, IT Governance and Information Security Governance to identify the possible components of this definition.

3. CORPORATE GOVERNANCE

Corporate Governance emerged as a discipline when the ownership of an organization was separated from its management. Governance, then, means protection of owners' interests through oversight, direction and control of management by owners, the owners being represented by the Board of Directors. Thus one of the main aspects of governance is to assure the suppliers of finance that they would get a return on their investments (Shleifer and Vishny, 1996, p. 3). Corporate Governance provides this assurance by providing incentives to the board and management to "pursue objectives that are in the interests of the company and its shareholders" (OECD, 2004, p. 13).

Moving forward from these philosophical underpinnings, guidance is available on the operational and implementation aspects of Corporate Governance. Corporate Governance is implemented through structures such as an organization's management, board, shareholders and other stakeholders that are bound by relationships. These structures and relationships are then utilized to set objectives and to determine the means of attaining those objectives and monitoring performance (OECD, 2004, p. 13).

A recent trend in the literature on governance of corporations or enterprises is towards taking a wider view of governance, i.e. Enterprise Governance with Corporate Governance being a part of it, or being synonymous with it. Figure 1 shows the Enterprise Governance Framework consisting of the conformance and performance dimensions (CIMA, 2004, p. 2).

The conformance dimension consists of the organization using its "governance arrangements to ensure it meets the requirements of the law, regulations, published standards and community expectations of probity, accountability and openness" (ANAO, 2003, p. 13). The conformance dimension includes Corporate Governance (CIMA, 2004, p. 2).

The performance dimension consists of the organization using its "governance arrangements to contribute to its overall performance and the delivery of its goods, services or programs" (ANAO, 2003, p. 13).

Operationally, Governance is "basically concerned with structures and processes for decision-making and with the controls and behaviour that support effective accountability for performance outcomes" (ANAO, 2003, p. 13).

Together, the conformance and performance structures and processes implement governance through "providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly" (Hamaker, 2003, p. 1).

From the above discussion, Governance can be understood to consist of the following aspects:

- It involves the Board of Directors and Executive Management.
- It makes the Board of Directors and Executive Management responsible towards all stakeholders including shareholders and suppliers of finance.
- It involves the creation of an organizational structure specifying the distribution of rights and responsibilities among the various participants in the organization.
- Governance includes the specification of processes for directing, controlling and monitoring performance of the organization towards attaining its objectives.
- Governance has conformance and performance aspects.
- The conformance dimension of Governance involves the formation of decision-making guidelines and structures and the clear identification and articulation of responsibilities.

- The performance dimension of Governance involves performance measurement and accountability for performance.

This section has investigated the meaning of governance. The following section investigates the definitions of IT Governance. Since, today, information largely exists in the IT devices deployed in organizations, it is instructive to look at what Governance means to IT to understand how it can be applied to Information Security.

4. IT GOVERNANCE

Information today is largely manifest in the electronic form. Also, today Information Security is largely about controls applicable to IT. This section investigates some definitions of IT Governance to understand what governance means to IT, in an attempt to understand what it can mean to cover Information Security. This paper does not see Information Security Governance as a subset of IT Governance as the drivers for IT Governance are very different from those for Information Security Governance.

The IT Governance Institute (ITGI) defines IT Governance as follows :

"IT Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives" (ITGI, 2003, p. 18).

Weill and Woodham (2002, p. 4) defines IT Governance as:

> "specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT".

Van Grembergen (2002, p. 1) defines IT Governance as:

> "the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensuring the fusion of business and IT".

The key point of the above definitions of IT Governance is that they see governance as a mechanism for fusing or aligning business and IT and getting value out of IT implementation. The definitions focus on the 'performance' outcomes of value creation and resource utilization. Likewise, the proposed definition of Information Security Governance should focus on the 'performance' outcomes of Information Security Governance and the value delivered by Information Security to the organization. However, the 'performance' outcomes and value delivered by Information Security Governance would be different from that of IT Governance.

5. EXISTING GUIDANCE ON INFORMATION SECURITY GOVERNANCE

This section investigates the guidance on Information Security Governance provided in the existing literature. This will help put in perspective the definition proposed in this paper.

The existing guidance on Information Security Guidance has two main themes:

- Motivating that Information Security must be governed and
- Defining Information Security Governance and providing guidance for implementation of governance.

The motivation for Information Security Governance is derived from the fiduciary responsibility of Board of Directors and Executive Management towards corporate governance and protection of stakeholder interests. It is motivated that not only are the Board of Directors and Executive Management responsible for maintaining information security, but also that they are liable for legal action for breaches in information security at their organization (von Solms, 2001) (von Solms and Thomson, 2003).

Since Governance consists of structures, relationships and processes, the existing guidance (ISACF, 2001) (CGTF, 2004) (BSA, 2003) (FISMA, 2002) provides frameworks for implementing Information Security Governance. The implementation proceeds mainly by mapping Information Security Governance responsibilities to the organizational hierarchy. A summary is provided in Table 1 – Information Security Governance and Organizational Hierarchy.

The existing guidance represents the beginning of a trend towards providing frameworks for Information Security Governance. The frameworks are therefore not sufficiently detailed and, in our opinion, would lead to a 'frustrated roll of eyes', as stated earlier. Further, the frameworks do not explicate a model or definition of Information Security Governance and are prescriptive in nature.

We attempt to remedy this shortcoming partially by proposing a definition of Information Security Governance in the next section.

6. PROPOSED DEFINITION OF INFORMATION SECURITY GOVERNANCE

This section proposes the following definition of Information Security Governance:

"Information Security Governance consists of the frameworks for decision-making and performance measurement that Board of Directors and Executive Management implement to fulfill their responsibility of providing oversight, as part of their overall responsibility for protecting stakeholder value, for effective implementation of Information Security in their Organization, to ensure that:

a. The Organization practices due care and due diligence in its use of Information and IT Systems and that this care and diligence is extended to its partners and customers.
b. The Organization manages the risks associated with its use of Information and IT Systems and that the process for Information Security is effective, efficient and responsive to security incidents and existing or emerging vulnerabilities, threats and risks.
c. The Organization's Information and IT Systems can be trusted by all stakeholders, including, customers, partners and regulators.
d. There is alignment between the needs and strategies of Business, IT and Information Security.
e. The Organization complies with laws and regulations applicable to its use of Information and IT Systems.
f. There is visibility into the state of Information Security in the Organization, providing relevant details to concerned stakeholders."

Figure 2 depicts a model of Information Security Governance, based on this definition. The following sections provide a brief discussion of the various components and characteristics of this definition.

7. THE 'GOVERNANCE' ASPECT OF INFORMATION SECURITY GOVERNANCE

This section discusses the 'Governance' aspect of the definition of Information Security Governance, i.e., what is meant by Governance, as it is applied to Information Security.

The definition states that Information Security Governance is a part of Enterprise or Corporate Governance and that the responsibility of Boards of Directors and Executive Management for providing oversight for protecting stakeholder interests includes providing oversight for implementation of Information Security.

The mechanisms for providing governance include creating the decision-making and performance measurement frameworks. These frameworks are formulated by the Board of Directors and Executive Management, but they are to be applied across all the layers of the organization. For the purpose of this discussion, an organization is modeled as consisting of the following layers :

- Corporate Governance Layer
- Executive Management Layer
- Operational Management Layer
- Technical Execution Layer

Thus, according to the definition, the decision-making and performance measurement frameworks are formulated by the top two layers, whereas the frameworks are applied across all 4 layers i.e. throughout the organization. Each of the four layers will, however, have its own requirements for what decisions are to be taken and what performance measures are to be monitored and reported.

As stated earlier in section 3 on Corporate Governance, the two frameworks will indeed be implemented through organizational structures. These structures will be related by their decision rights, responsibilities and accountabilities and the structures will operate as per the defined processes. These details will form the two frameworks.

The formulation of the Decision-making framework will be guided by questions such as:

- What are the decisions to be taken?
- Who takes which decision?
- What process is to be followed?
- What are the standards, policies, guidelines etc. that are needed to guide decision-making?
- What are the checks, controls and balances for ensuring proper decision-making?

The formulation of the Performance-Measurement framework will be guided by questions such as:

- Who are the stakeholders and what value do they expect from Information Security?
- Are our decisions being implemented and to what extent?
- What metrics do we need to monitor and report?

The approach to applying governance to information security would then mean asking and answering the above questions, and many more such questions, as they apply to information security e.g.

- What does information security mean for us?
- How much security do we need ? What is our risk appetite?

- Who will decide information security project prioritization and budgeting?
- How do we ensure alignment between Business, IT and Information Security?
- What support do Information Security projects need from the organization?
- What is our security architecture?
- Etc.

In the next section, the value that governance will enable information security to deliver to the organization gets discussed.

8. THE 'PERFORMANCE' OUTCOMES ASPECT OF INFORMATION SECURITY GOVERNANCE

This section discusses the 'performance' outcomes aspect of the definition of Information Security Governance i.e., the value that governance allows Information Security to deliver to the organization. The value ranges from being an effective protective mechanism to strategic alignment between the needs of business and information security.

The first three 'performance' outcomes of Information Security Governance can be seen as a hierarchy:

a. Due care and due diligence in the use of Information and IT Systems i.e. a healthy control environment which is the base foundation,
b. An effective and efficient process with due commitment and allocation of resources which leads to ... (the next higher layer mentioned below),
c. Internal and external trust in the organization's information and IT systems.

Information Security Governance has to ensure that appropriate entities are responsible for decision-making and accountable for performance measurement for delivering on the above objectives.

Another important aspect of information security implementation in organizations is the alignment that must be achieved between business, IT and information security. Information Security Governance has a crucial role in ensuring this alignment – not only must information security satisfy business and IT needs, but business and IT must conform to security guidelines. Information Security Governance delivers on alignment by ensuring that business, IT and information security participate in relevant decision-making and that appropriate performance metrics are defined.

Information Security is increasingly being regulated with many legislations and regulations being applicable. Information Security Governance has to ensure that the compliance posture of the organization is identified and that the appropriate regulations are complied with accordingly.

A major requirement for governance is to ensure reporting of relevant details to stakeholders. The purpose of this reporting is to ensure that stakeholders have visibility into the health of the organization. Information Security Governance has to ensure that the stakeholders are identified and their information needs are satisfied.

In this section, the elements of the value that information security delivers to the organization has been identified. Information Security Governance has a vital role in enabling this value delivery.

9. CONCLUSION

In this paper, a definition of Information Security Governance, based on a review of the current literature on Corporate Governance, IT Governance and Information Security Governance, was provided. This definition has two parts viz. the governance aspect and the value aspect. The definition links these two aspects together to show how governance can enable information security to deliver value to the organization.

The proposed definition is comparable to the definition of 'Internal Control' as proposed by (COSO, 1992) which defines 'Internal Control' as the responsibility of Board of Directors and Executive Management. The objectives of 'Internal Control' are effectiveness of operations, reliability of financial reporting and compliance with applicable laws and regulations (COSO, 1992). Likewise, the proposed definition is comparable to the 'Security Organization' control contained in ISO 17799 (ISO 17799). This control envisages a management framework consisting of allocation of responsibilities, co-ordination and approval processes. However, ISO 17799 does not provide any detailed framework for the implementation of this control.

The definition can serve as a foundation for developing a framework for Information Security Governance in organizations. This framework can then be used by Board of Directors and Executive Management to implement effective Information Security within their organization.

10. REFERENCES

ANAO (2003). Public Sector Governance Volume 1 Better Practice Guide Framework, Process and Practices. *Australian National Audit Office*. (online) (cited 05 May 2005). Available from Internet: URL http://www.anao.gov.au/WebSite.nsf/0/957e55a69b1050724a256d73001dfd1c/$FILE/Volume%201,%20Framework,%20Processes.pdf

BSA (2003). Information Security Governance: Toward a Framework for Action. *Business Software Alliance.* (online) (cited 05 May 2005). Available from Internet: URL http://www.bsa.org/resources/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=5841&hitboxdone=yes

CGTF (2004). Information Security Governance: A Call To Action. *Corporate Governance Task Force.* (online) (cited 05 May 2005). Available from Internet: URL http://www.cyberpartnership.org/InfoSecGov4_04.pdf

CIMA (2004). Enterprise Governance Getting the Balance Right Executive Summary. *Chartered Institute of Management Accountants.* (online). (cited 05 May 2005). Available on Internet: URL http://www.cimaglobal.com/cps/rde/xbcr/SID-0AAAC564-30AB5F4F/live/enterprise_governance_summary_2004.pdf

COSO (1992). Internal Control - Integrated Framework Executive Summary. *The Committee of Sponsoring Organizations of the Treadway Commission.* (online). (cited 05 May 2005). Available from Internet: URL http://www.coso.org/publications/executive_summary_integrated_framework.htm

FISMA (2002). Federal Information Security Management Act of 2002. *U.S. Congress.* (online). (cited 05 May 2005). Available from Internet: URL http://csrc.nist.gov/policies/FISMA-final.pdf

Hamaker, S. (2003). Spotlight on Governance. *Information Systems Control Journal,* Volume 1, 2003. (online). (cited 05 May 2005). Available on Internet: URL http://www.shamrock-technologies.com/Journal_article2.pdf

ISACF (2001). Information Security Governance: Guidance for Boards of Directors and Executive Management. *Information Systems Audit and Control Foundation.* (online). (cited 05 May 2005). Available on Internet: URL http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Information_Security_Governance_Guidance_for_Boards_of_Directors_and_Executive_Management/infosecurity.pdf

ISO 17799. ISO / IEC 17799:Code of Practice for Information Security Management. *International Standards Organisation, Geneva, Switzerland.*

IT Governance Institute (ITGI) (2003). Board Briefing on IT Governance, 2nd Edition. *IT Governance Institute.* (online). (cited 05 May 2005). Available on Internet: URL http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=4667

Melnicoff, Richard M., Shearer, Sandy G. & Goyal, Deepak K. (2005). Is There a Smarter Way to Approach IT Governance ? (online). (cited 05 May 2005). Available from Internet: URL http://www.accenture.com/xdoc/en/ideas/outlook/1_2005/pdf/it_gov.pdf

OECD (2004). OECD Principles of Corporate Governance. *Organisation For Economic Co-operation and Development.* (online). (cited 05 May 2005). Available on Internet: URL http://www.oecd.org/dataoecd/32/18/31557724.pdf

Shleifer, Andrei and Vishny, Robert W. (1996). A Survey of Corporate Governance. *NBER Working Paper No. W5554.* (online). (cited 05 May 2005). Available on Internet: URL http://papers.nber.org/papers/w5554.pdf

Van Grembergen, W. (2002). Introduction to the Minitrack: IT governance and its mechanisms. *Proceedings of the 35th Hawaii International Conference on System Sciences (HICCS), IEEE.* (online). (cited 05 May 2005). Available on Internet: URL http://www.hicss.hawaii.edu/HICSS39/foscfp.htm

von Solms, Basie (2001). Corporate Governance and Information Security. *Computers & Security 20(3): 215-218 (2001).*

von Solms, R., & Thomson, Kerry-Lynn (2003). Integrating Information Security into Corporate Governance. *IFIP TC11, 18th International Conference on Information Security (SEC2003), Athens, Greece.* Kluwer Academic Publishers Group, Netherlands : pp. 169-180.

Weill, Peter & Woodham, Richard (2002). Don't Just Lead, Govern: Implementing Effective IT Governance. *MIT Sloan Working Paper No. 4237-02.* (online). (cited 05 May 2005). Available from Internet: URL http://ssrn.com/abstract=317319

Table 1. Information Security Governance and Organizational Hierarchy

(ISACF, 2001)	(CGTF, 2004)	(BSA, 2003)	(FISMA, 2002)
• Board • Management	• Board of Directors / Trustees • Senior Executive • Executive Team Members • Senior Managers • All Employees and Users	• Corporate Executives • Business Unit Heads • Senior Managers • CIOs / CISOs	• CEO • Business Unit Heads • Senior Managers • CIO / CISO

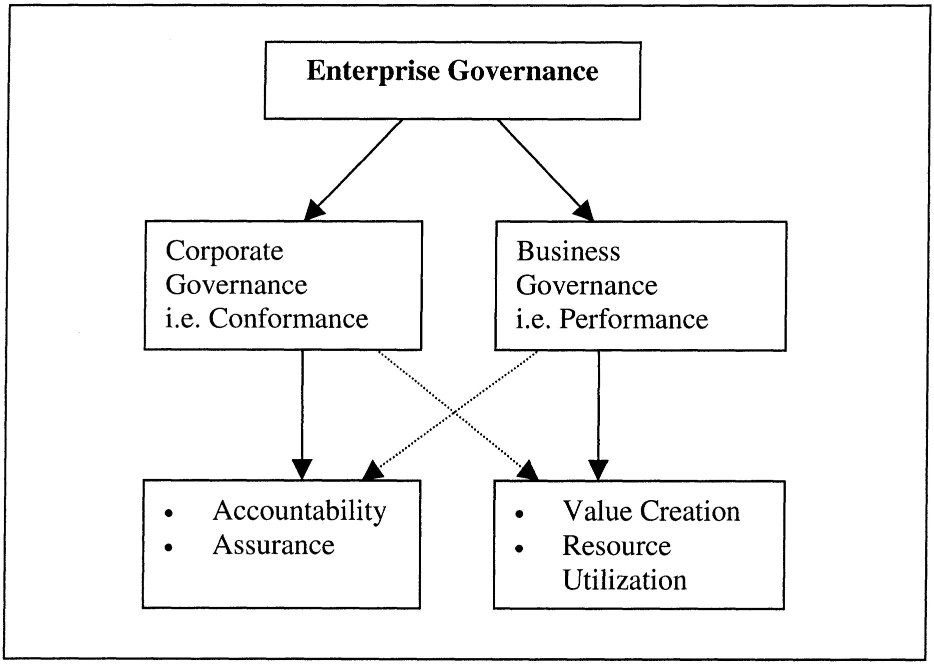

Figure 1. The enterprise governance framework (CIMA, 2004)

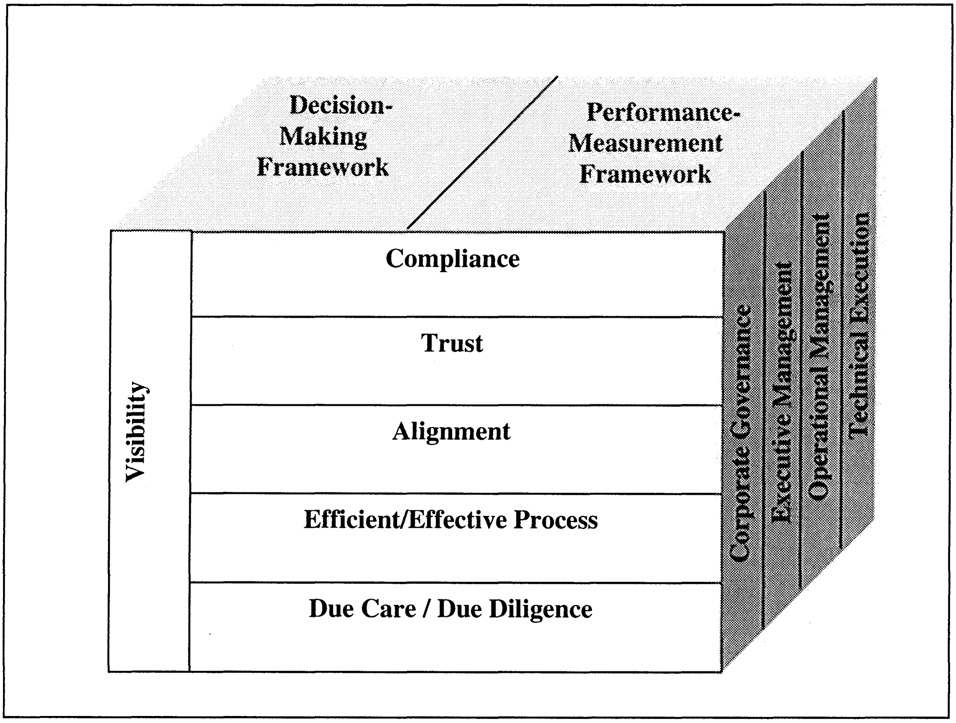

Figure 2. Information Security Governance Model