Chapter 1
Overview of Key Information Security Governance Frameworks

Oscar Rebollo
Ministry of Labour and Immigration, Spain

ABSTRACT

Security awareness has spread inside many organizations leading them to tackle information security not just as a technical matter, but from a corporate point of view. Information Security Governance (ISG) provides enterprises with means of dealing with the security of their information assets in a comprehensive manner, involving every stakeholder through the whole governance and management processes. Boards of Public and Private Entities cannot remain unaware of this development and should make efforts to include ISG into their business processes. Realizing of this relevant role, scientific literature contains a variety of proposals which define different frameworks to foster ISG inside any corporation. In order to facilitate the adoption of any of them by the public sector, this chapter compiles existing approaches, highlighting the main contributions and characteristics of each one. Senior executives and security managers may need support on their decisions about adopting one of these frameworks, so a comparative analysis is performed. This chapter tries to provide an overview of state of the art of the most current relevant security governance frameworks by means of a comparison through a set of comparative criteria that have been defined and applied to every proposal, so that strengths and weaknesses of each one can be pointed out. These criteria have been selected from a deep analysis of existing ISG papers, including both governance and management aspects.

DOI: 10.4018/978-1-4666-2083-4.ch001

INTRODUCTION

As results show, each proposal mentioned in the abstract focuses on different aspects of ISG giving priority to some of the defined criteria, and none of them covers the entire required spectrum. Most of the selected frameworks can be used by any public or private organization as a starting point towards integrating security inside their processes, but this paper helps managers to be aware of its limitations and the gaps which need to be covered in order to achieve a complete integration. Special attention has been given to public sector due to the importance of security on this sector.

Consequently, more investigation is needed to fulfill detected gaps and define an ISG framework that organizations can rely on, and which offers security guarantees of covering every information asset of the company.

Information Technology (IT) security can no longer be considered as a technical issue that can be assessed through hardware implementations, but it is a process that involves the whole company (Pasquinucci, 2007). It is widely accepted that security needs to reach the governance level so that senior directors understand the risks and the opportunities, and have assurance that these are being properly and continuously managed (Williams, 2001). The motivations to introduce IT in the corporate executive agenda is twofold: many countries have developed legislation to hold responsibilities for security breaches (BSA, 2003, Hardy, 2006), and achieving a higher security degree may become a competitive advantage to the organization (Humphreys, 2008, Johnston and Hale, 2009).

Public entities are also involved with these considerations, as higher IT security usually strengthens the trust relationship between Administrations and their citizens. A recent European Union research shows existing gaps related with security and privacy concerns that need to be fulfilled in the field of electronic governance and policy modeling (Crossroad, 2010).

All these objectives may be achieved through Information Security Governance (ISG) which is an overarching category directly affecting the entire policy management process (Knapp et al., 2009). There is not a unique definition of ISG, but among the most widespread conceptions it is generally accepted that ISG consists of the leadership, organizational structures and processes that safeguard information (ITGI, 2006b). ISG can also be defined more specifically as the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk (Bowen et al., 2006). Finally, focusing on the stakeholders' roles, ISG 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 (Rastogi and Solms, 2006).

In order to secure their information assets, companies need to adopt an ISG framework that assures effective implementation and makes process operational (Corporate Governance Task Force, 2004). Although there exist a variety of proposed frameworks, organizations neither know which one to adopt nor which one tailors to their own necessities. To help managers in their decisions, the following three comparative reviews have been found: (Rastogi and Solms, 2006) provide existing guidance on ISG and use four frameworks to propose a new definition of ISG; (Park et al., 2006) develop a literature review to