Chapter 15

Information Security Governance and Standard Based Management Systems

Margareth Stoll
University of Innsbruck, Austria

Ruth Breu
University of Innsbruck, Austria

ABSTRACT

The importance of information and Information Systems for modern organizations as a key differentiator is increasingly recognized. Sharpened legal and regulatory requirements have further promoted to see information security governance as part of corporate governance. More than 1.37 million organizations worldwide are implementing a standards based management system, such as ISO9001 or others. To implement information security governance and compliance in an effective, efficient, and sustainable way, the authors integrate these standard based management systems with different information security governance frameworks and the requirements of the international ISO/IEC 27001 information security management standard to a holistic information security governance model. In that way information security is part of all strategic, tactical, and operational business processes promotes corporate governance and living information security. The implementation of this innovative holistic model in several organizations and the case studies results are described.

INTRODUCTION

Due to globalization and increasing competition, information and supporting technology have become key asset and differentiators for modern organizations. Organizations and their information and information systems are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. 92% of large enterprises had a security incident in the last year with an average cost of 280,000-690,000 £ for the worst incident (PricewaterhouseCoopers, 2010). Mobile
Information Security Governance and Standard Based Management Systems

and cloud computing, off-shoring, social networks and the increasingly interconnected, flexible and virtualized business complexity and dependencies are still great challenges for existing information security governance.

In the last years, the legal and regulatory requirements in this area have been sharpened. Most modern corporate governance guidelines, and always more laws, make the board and specifically the CEO responsible for the well-being of the organization. Lack of security compliance may result in loss of confidence of customers, partners and shareholders, as well as severe civil and criminal penalties for board members (Saint-Germain, 2005; Clinch, 2009). More and more organizations are reducing their business risks by seeking assurance that their supplier and partners are properly protecting information assets and ensuring business continuity (Saint-Germain, 2005). In this respect the availability of all essential assets, confidentiality, data integrity and legal and regulatory compliance are central for organizations’ success and integral part of good IT and corporate governance (Da Veiga & Eloff, 2007; Solms & Solms, 2009; Sowa, Tsinas & Gabriel, 2009). This poses great challenges for small and medium sized organizations. They need a very efficient and functional approach, which can be smoothly integrated in their daily business.

Several international best practices for information security management have been developed to provide guidance and ensure comprehensiveness. Some of the most commonly used include Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL) and national guidelines, such as NIST SP 800 series in the US or IT Security Guidelines from the Federal Office for Information Security in Germany. More than 12.934 organizations worldwide have just implemented an information security management system in accordance to ISO/IEC 27001 (International Standard Organization [ISO], 2010). This international standard provides a model for establishing, operating, monitoring, maintaining and improving an information security management system to meet the specific security and business objectives of the organization. Thereby the organization’s overall business strategy, objectives and requirements, the legal, statutory or regulatory requirements and the contractual security obligations, as well as the organization’s business risks, processes and procedures are taken into account (ISO, 2005a; 2005b).

More than 1.37 million organizations of different sizes and scopes have implemented management systems based on international standards (e.g. quality ISO 9001, or environment ISO 14001, IT service management ISO 22000 and others) (ISO, 2010). All these management systems require common principles: the establishment and communication of organization objectives and strategies, the management of business processes, an adequate resource management and the continual improvement of the organization (ISO, 2008). The management system must be documented, communicated, implemented and continuously improved. These systems are implemented more frequently in a holistic way. According with the organizational purpose and objectives different aspects, like quality, environment, hygiene, social, occupational health and safety or others are integrated.

To meet optimally all information security requirements and compliance we have developed an efficient, effective and sustainable information security governance model. The innovation of this information security governance model is the integration of different information security governance frameworks with the ISO 9001 standard for quality management systems or other international standards for management systems, as well as with the international standard for information security management IEC/ISO 27001 and best-