Managing Compliance with an Information Security Management Standard

Heru Susanto
School of Business and Economics, University of Brunei Darussalam, Brunei Darussalam & The Indonesian Institute of Sciences, Indonesia

Mohammad Nabil Almunawar
School of Business and Economics, University of Brunei Darussalam, Brunei Darussalam

INTRODUCTION

Compliance to an Information Security Management System (ISMS) Standard is an effective way to manage information security within an organization. Unfortunately, the task to implement compliance to an ISMS standard is not easy as the description and requirements of a standard are normally complex and difficult to understand. Many US information and communication technology (ICT) projects, including ISMS standardization and ISO 27001 compliance projects, in major organizations faced difficulties and many reported failure and lost billions of dollars (SG, 2003). For example, BCS Review (2001) found that only around one in eight (13%) of ICT ISO 27001 standardization projects were successful implemented. Schwalbe (2010) and Heeks (2003) stated that technical barriers, project owner's absence of understanding-processes, technically savvy aspects, lack of internal ownership, and neglected certain aspect, are major problems that cause the delay for ISMS and ISO 27001 projects.

However, it cannot be denied that information security has a very important role in supporting and enabling activities of the organization (Solmn, 2008) and compliance to an ISMS standard is important. Therefore, there is a need to have a framework that can map the standard systematically to avoid failures and lengthy implementation of ISMS standardization projects

One of the key components to understand the process and technical savvy aspects of an ISMS such as ISO 27001 is to use a framework to map the detail components of ISO 27001 systematically. There are several frameworks available, however, these frameworks are difficult to use and do not provide measurable variables for readiness and information security capabilities (RISC) measurements. The RISC measurements are investigation stages to find out organization's readiness and information security capabilities over the ISO 27001.

In order to solve complex and challenging problems for the implementation of ISO 27001, particularly in dealing with technical issues of information security and compliance processes, a new framework, integrated solution framework (ISF), is discussed in this article. ISF is developed to provide an abstraction and mapping of the ISO 27001 controls for RISC investigations.

ISF is designed in such a way to overcome technical issues faced by organizations to pursue ISO 27001 compliance projects efficiently. Compliance to an ISMS standard such as ISO 27001, which is also called *information security assessment,* is a process of comparing security-related controls done by an organization with those in the standard. It is a gap analysis in which the differences between information security circumstances of an organization with the standard are discovered. The task of checking conformity level helps an organization to determine its relative position to the standard, which is very useful for a certification process.

This article discusses issues for effective and efficient management for compliance with ISMS (ISO 27001). The next section will present the background followed by a literature review on existing frameworks. A new framework is discussed in the following section. The last two section are future directions the conclusion respectively.

DOI: 10.4018/978-1-4666-5888-2.ch138

BACKGROUND

The rapid advancement of ICT and the growing dependency of organizations on ICT intensify concern on information security (Solms, 2001). Although most ICT systems are designed to have a considerable amount of strength in order to sustain and assist organizations in protecting information from security threats, they are not immune from those threats. Organizations are increasingly paying attention to information protection as the impact of information security breaches today have more tangible effects (Dlamini et al., 2009).

The ever-changing business environment poses new vulnerabilities on information assets. These vulnerabilities will increase the possibility of security breach or attack by hackers (Anderson, 2006; Dhillon, 2007). Cyber criminals keep adapting their techniques to exploit vulnerabilities. As a result, cybercrime is becoming more common (Aceituno, 2005; Easttom, 2007). Consequently, the number and cost of security breaches appears to be rising fast (ISBS, 2010).

Information security breaches within organizations were reported by ISBS (2012), which stated that '*incidents caused by staff*' was experienced by 82% of the sampled large organizations. No industry sector appears immune from these incidents. Telecommunications, utilities, and technology companies appear to have the most reliable systems. The public sector, travel, leisure, and entertainment companies are most likely to have security problems. Moreover, it was found that the average security incident within local business organisations occurred once a month, while large or international organizations would expect an incident to occur once a week (ISBS, 2012).

Thomas (2003) estimated that the total loss caused by the work of computer hackers and viruses was about £1trillion. In addition, because of weak protection, leaks of confidential information can result in inappropriate publicity for an organization. This may lead to loss in business as customers lose their confidence to transact (Anderson, 2001).

Pollitt (2005) indicated that 70% of IT budgets were spent after experiencing a security breach. As such, organizations use new ways to prevent information security breach and threats, through the concept of *five principles of security*, which are: planning, proactive, protection, prevention, and pitfalls. *Five principles of security* are used to identify signs and flags of intruders in a network, establish guidelines for safeguarding user names and passwords, and protect against physical access to information technology facilities.

It is clear that information security needs to be managed properly as the issues are quite complex. As such, several ISMS standards were developed to assist organizations in managing the security of their information system assets. It is important to adopt an ISMS standard to manage the security of information assets effectively.

To conform to an ISMS standard such as ISO 27001, organizations have to conduct an information security assessment. According to Kosutic (2013), the information security assessment is probably the most complex and challenging part of an ISO 27001implementation project. However, it is the most important step toward the adoption of an ISO 27001. An information security assessment is basically a process to lay the foundations to find out the occurrence of potential incidents (i.e. assessment of risks) (Alfantookh, 2009) and to address the most appropriate way to avoid such incidents by referring to the associated controls (i.e. treating the risks) (Calder, 2006).

LITERATURE REVIEW

There are nine frameworks available to help, abstract and organize efforts to comply with information security standards. Those frameworks are (1) a framework for the governance of information security (Posthumus & Solms, 2004), (2) a framework for information security management based on guiding standard: a United States perspective (Sipior & Ward, 2008), (3) a security framework for information systems outsourcing (Fink,1994), (4) information security management: a hierarchical framework for various approaches (Eloff & Solms, 2000), (5) information security governance framework (Ohki et al., 2009), (6) Queensland government information security policy framework (QGISPF, 2009), (7) STOPE methodology (Bakry, 2004), (8) a security audit framework for security management in the enterprise (Onwubiko, 2009), (9) multimedia information security architecture framework (Susanto & Muhaya, 2010).

Framework for the governance of information security (FGIS) was introduced by Posthumus and Solms (2004), which revealed and suggested the important