Chapter 22
Three Models to Measure Information Security Compliance

Wasim A. Al-Hamdani
Kentucky State University, USA

ABSTRACT

This work introduces three models to measure information security compliance. These are the cardinality model, the second’s model, which is based on vector space, and the last model is based on the priority principle. Each of these models will be presented with definitions, basic operations, and examples. All three models are based on a new theory to understand information security called the Information Security Sets Theory (ISST). The ISST is based on four basic sets: external sets, local strategy sets, local standard sets, and local implementation sets. It should be noted that two sets are used to create local standard sets—local expansion and local creation. The major differences between the Zermelo Fraenkel set theory and the ISST are the elimination of using empty element $\phi$ and empty set. This assumption is based on “there is not empty security” measure and the $\phi$ is substituted to be $\lambda$ and is defined as “minimum security (or system default security)”. The main objective of this article is to achieve new modeling system for information security compliance. The compliance measurement is defined in the first model as the cardinality between local strategy sets and the actual local implementation. The second model is looking at the security compliance as the angle $\theta$ between two sets, local implementation and local standard. The third model is based on the priority philosophy for local security standard.

1. INTRODUCTION

Compliance is one of the major issues in information security management is “to be sure been evaluated correctly”. Compliance (regulation) is defined as, “the act of adhering to, and demonstrating adherence to, a standard or regulation” (Wikipedia.org, 2008) or “Conformity in fulfilling official requirement” (MerriamWebster.com, 2009). Many industries measure the compliance with best practices as compliance with ISO 17799 or NIST special publication 800. A normal procedure to
Three Models to Measure Information Security Compliance

measure compliance is to create a checklist and label two elements finding and compliance, such as in BS 7799.2:2002 Audit Checklist (Thiagarajan, 2003) or ISO 17799 checklist (Thomas, 2003). The checklist evaluator would give either a value of 1 (for YES) to element compliance and 0 (for NO) for noncompliance and the final result measured mathematically would be: “

Superior: >95 “yes” answers
Fair: 82–95 “yes” answers
Marginal: 68–81 “yes” answers
Poor: 54–67 “yes” answers
At Risk: <54 “yes” answers”

Such a model can be mathematically summarized as the sum for all elements $\sum_{i=1}^{n} x_i$ and $x_i$ is an element in the security list.

Another issuer is to look at compliance through regulation. As Adler (2006) pointed out, “Self-regulation through the implementation of good security practices was thought to be the way to protect electronic personal information. In the latter part of the 20th century, “a sectoral approach to information security regulation started to gain favor with the passage of laws protecting health and financial information” (Adler, 2006). Most regulation compliance is with:

- Health Insurance Portability and Accountability Act (HIPAA) compliance,
- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standard (PCIDSS)
- Federal Information Security Management Act of 2002 (FISMA)
- OMB M-06-16 addresses the protection of agency information that is either “accessed remotely or physically transported outside of the agency’s secured, physical perimeter” (Adler, 2006).

Some have permitted information security compliance to be handled by more than one department. For example, in education campuses (Adler, 2006), the university hospital or the health center may be tasked with Health Insurance Portability and Accountability Act (HIPAA) compliance, the financial aid office or departments using credit cards may focus on compliance with the Gramm-Leach-Bliley Act (GLBA) or the Payment Card Industry Data Security Standard (PCIDSS), while the registrar may be held responsible for the privacy of student educational records under the Family Educational Rights and Privacy Act (FERPA).

On the technical level, many organizations reference their technical (configuration) standards compliance based on NIST special publications 800 series and NIST checklist (NIST, 2008). As in Special Publication 800-70, “A security configuration checklist (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of documented instructions for configuring a product to a pre-defined operational environment. It could also include templates or automated scripts and other procedures. Checklists can be developed for specific IT products and environments not only by IT vendors, but also by consortia, industry, Federal agencies and other governmental organizations, and others in the public and private sectors. The use of well-written, standardized checklists can reduce the vulnerability exposure of IT products and be particularly helpful to small organizations and individuals for securing their systems” (Soupaya, Wack, & Kent, 2005, p. 1).

To summarize these issues, there are two types of compliance measures:

- Using baseline or best practices in the industry or best standards (as using ISO