Regulatory Compliance in Information Technology and Information Security

Herbert Mattord
Kennesaw State University

Michael Whitman
Kennesaw State University

Follow this and additional works at: http://aisel.aisnet.org/amcis2007

Recommended Citation
http://aisel.aisnet.org/amcis2007/357

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Regulatory Compliance in Information Technology and Information Security

Herbert J. Mattord, CISSP and Michael E. Whitman, Ph. D., CISSP
Kennesaw State University
hmattord@kennesaw.edu & mwhitman@kennesaw.edu

ABSTRACT
This paper serves as the introduction and operating guide for the AMCIS 2007 mini-track on Regulatory Compliance in Information Technology and Information Security. It provides a description of the mini-track, a discussion of its importance and relevance in the field of Information Systems, a descriptive list of the areas of coverage that the mini-track seeks to pursue. It also provides a brief glossary of key terms that can serve to add clarity to the researchers who are engaged in work in this area and provides a recap of the topics that have been covered in past conferences. It concludes with a short list of comments on future directions for research on this topic.

Keywords
Regulatory compliance, regulations, laws, standards.

INTRODUCTION
This mini track will allow for the sharing of knowledge and perspectives and encourage research in the areas of government regulation and industry standards that apply to the information technology and information security industries. Government regulations have and will continue to be required by jurisdictions around the world. Industry and trade groups attempt to direct the response to these regulatory environments by developing and adopting standards and recommended practices that seek to improve alignment with a variety of objectives. Most organizations that employ IT systems are struggling with mechanisms to assure compliance with regulations and/or conformance to industry standards.

IMPORTANCE AND RELEVANCE
Recent years have seen an added number of important new regulations that apply to the IT industry. Practitioners have seen significant impacts in the prioritization of projects within their organizations as they scramble to achieve compliance with both government regulations and industry standards. Recent trends indicate this will continue to be an issue for practitioners and seems to indicate a need for added emphasis from the academic community.

AREAS OF COVERAGE AND TOPICS OF INTEREST
The following areas and topics have been identified by researchers participating in this mini-track as being of interest for ongoing work:

Laws:
- Impact of Sarbanes-Oxley on IT Project Funding
- HIPAA impacts on IT Systems Development Projects
- Integrating HIPAA/SarBox/GLB Requirements into system design specifications

Regulations:
- Developing systems to support the Customs Trade Partnership Against Terrorism
- Systems Design Impacts of European Union Privacy Directives
- Economic Impacts of IT Regulation

Standards:
TERMINOLOGY

The following terms have been used in this area of interest and are offered here to clarify their intended meaning in the context of this mini-track:

- **Law** – The regulations established in a community by a recognized authority and applicable to those who live and/or work in that community. May be explicitly defined as in the form of legislation or it may be less formal as in a custom recognized and enforced by judicial decision.
- **Regulation** – Directives from a recognized authority that direct the actions of individuals or groups to achieve conformance with the intentions of those in power in a given jurisdiction. Regulations are generally founded in law and their application will be tested by the interpretation of the underlying law.
- **Standard** – A method or process that is considered by an entity or group perceived as having some authority as a basis of comparison so that others may follow that example as an approved model.
  - **Compulsory Standard** – A standard to which an organization must comply in order to avoid the imposition of some form of sanction.
  - **Voluntary Standard** – A standard to which an organization may comply at its own discretion.
- **Global Business Regulation** – Global business regulation has been defined by Pattberg “limits imposed on the behavior of economic actors contained in rules and standards”. [1] Recent actions by governments and supra-governmental organization have added new emphasis for this topic to organizations that operate on an international scale.
- **Jurisdiction** – The authority, based on law, to administer justice or settle disputes between parties.

PAST CONFERENCES

AMCIS 2006 was the first time this mini-track has taken place. The papers presented were:

- Anti-Phishing Strong Authentication Technology Options, Paul Witman, Claremont Graduate University.
- Compliance–Appropriate Spreadsheet Testing, Raymond Panko, University of Hawaii.
- IT Governance and the Sarbanes-Oxley Act, Michael Leih, Claremont Graduate University.

CURRENT CONFERENCE

AMCIS 2007 marks the second time this mini-track has taken place. The papers scheduled to be presented are:

- The Influence of Regulations On Innovation In Information Security, Lara Khansa and Liginlal, Divakaran, University of Wisconsin.
- Banking Regulatory Response – the Case of Strong Authentication, Paul Witman, California Lutheran University.

FUTURE RESEARCH

At present this mini-track and its areas of interest are not receiving the benefit of any coordinated efforts to synchronize the research activities of contributors. While the general area is perceived as having a need for more in the way of data collection, conceptual model building and model validation, little has been done in any coordinated fashion.
There is a need to clearly distinguish among regulations that currently encompass firms who consume IT and firms who produce IT and Information Security products and services. The issue of regulating IT has been discussed at several Conferences designed for practitioners as well as the work being done at academic conference. It would be useful to coordinate these efforts.

What are the publishing outlets for research in this area? How can information security journals be brought into the list of recognized Information system publications for the purposes of tenure? It would be a useful effort to create a central catalog of publishing outlets for this topic area.

While there is a need for more data collection, conceptual model building and model validation, can something be done to begin the formation of some type of organization to collect data from firms and serve as an authoritative repository of data related to the impact of information security regulations? Is there a privacy breach database similar to that of CERT that one can rely upon? This topic is of sufficient important to industry it may be possible to coordinate efforts towards more data collection and validation with benefits that will certainly go beyond academia to actually assist industry.

An initial project would be to develop a review of recent literature on the various topics in the list of areas and topics itemized above. Once this is complete, a subset of the areas can be examined in greater detail to suggest specific topics that might benefit from future efforts and collaborative activities.
REFERENCES