Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Regulatory Impact on IT Governance: A Multiple Case Study on the Sarbanes-Oxley Act

Michael Leih
Claremont Graduate University

Regulatory Impact on IT Governance: A Multiple Case Study on the Sarbanes-Oxley Act

Michael Leih
Doctoral Candidate
School of Information Systems and Technology
Claremont Graduate University
michael.leih@cgu.edu

Introduction

This study will evaluate how certain types of regulatory changes are impacting Information Technology (IT) governance. Most laws and regulations impacting IT have focused on data privacy. Laws such as the Children's Online Privacy Protection Act (CORPA), the Health Insurance Portability and Accountability Act (HIPPA), and the California Online Privacy Protection Act (OPPA) are examples of regulatory requirements that have mandated organizations to protect the personal information they are entrusted with. Even industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS), focus their attention on mandating organizations to protect the personal information of clients and customers. The impact of these data privacy laws and standards to IT organizations have been limited to the ways companies must handle and store personal information, but have not significantly changed the way IT organizations are governed. However, a few recently passed regulations are impacting the overall IT governance in many organizations. This change to IT governance has been significant in many instances but little theory has been developed to evaluate or study the regulatory impact to IT governance (Leih 2006). The Clinger-Cohen Act (USA), the Basel II Accord (Europe), and The Sarbanes-Oxley Act (USA) are all examples of recently enacted regulations that have greatly impacted the entire IT organization and have changed the structure of IT governance (Bonham 2005).

Weill and Ross (2004) define IT governance as "Specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT. The IT Governance Institute adds to this definition by including the idea of the organization through the phrase "… the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives". (IT Governance Institute 2003) These definitions provide the context of how IT governance will be viewed throughout this study.

The Clinger-Cohen Act of 1996 impacts the majority of U.S. federal agencies by mandating that each IT department implement a more formal IT portfolio management practice. In addition, the Act requires that each government agency's IT organization must coordinate their management policies and practices with other government and public agencies (U.S. Congress 1996). The Basel II Accord revises the international standards for measuring the adequacy of a bank's capital through risk assessment. It primarily impacts European financial institutions by regulating risk management across national boarders. IT organizations within financial institutions are required to manage their risk contribution by assessing potential losses due to IT systems and IT staff processes (Broadbent and Kitzis 2005). The Sarbanes-Oxley Act of 2002 impacts all SEC registrants, including all U.S. public companies, some private companies registered with the SEC, and all foreign companies trading on a U.S. exchange. Among several requirements, the Act mandates that companies implement internal controls to ensure accurate finical reporting. Because of the tight integration between financial reporting and IT, the impact to IT governance has been significant in many public companies (U.S. Congress 2002).

There has been limited research in the area on how regulatory requirements are impacting IT governance. However, with passage of the aforementioned regulations, this area of research is worth considering. Because of the limited research, an exploratory multiple case study approach is being selected as one appropriate way to study the impact of regulatory changes to IT governance (Yin 2003). This study will focus on the Sarbanes-Oxley Act as the regulatory initiative because of its broad impact in several business areas. Three small to medium sized companies have been selected to participate in the study because there is prior research showing that smaller companies are experiencing a greater degree of change and should provide more vivid examples of the type and degree of impact (Leih 2006).

Theoretical Model

Yin (2003) suggests that when conducting a case study to develop new theory, the researcher should explore the relevant prior literature and theories to provide some structure to data gathering and analysis. Because the impact of regulatory change to IT governance can be primarily seen as a process change to the IT organization, this study will be framed using process change theory as a foundation to develop a new theoretical model. Van de Ven and Poole (1995) have identified four theories, or "motors", that serve as building blocks for explaining the process of change in an organization: life cycle, teleology, dialectics, and evolution. Each of these theories describes different progressions of change events that are driven by different forces and operate at different levels within an organization. In addition, each of these theories is part of the larger family of process theory focusing on organizational transitions through events and activities that occur over time (Cule and Robey 2004). Of these four, the teleological motor appears to provide the most appropriate framework through which to analyze the organizational change caused by a regulatory mandate, such as the Sarbanes-Oxley Act.

The teleological motor has been used in several case studies as a framework through which to interpret the changes an organization is experiencing (de Rond 2004; Doz 1996; Pare 2002). In addition, other papers have referenced teleology as an appropriate foundation for determining the cause of change and a model through which to evaluate the study of organizational transitions (Cule and Robey 2004; Hooker 2004). The mode of change associated with teleology is considered to be constructive. A constructive mode of change typically creates unique and innovative forms that are often considered to be unpredictable and discontinuous departures from past activities (Van de Ven and Poole 1995). This mode of change is not described as deterministic, but rather emergent as the change process unfolds. Van de Ven (1992) explains that the model incorporates the systems theory assumption of equifinality; that there are several equally effective ways to achieve the given goal.

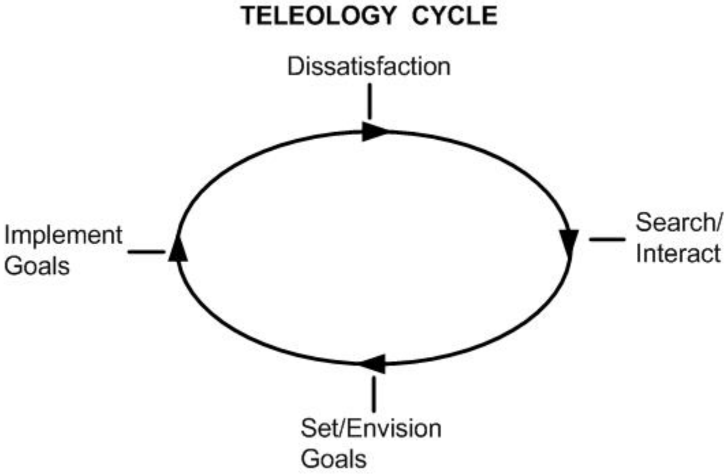

Figure 1: Teleological Cycle (Adapted from Van de Ven and Poole 1995)

Van de Ven and Poole (1995) define the teleological process of organizational development and change as a continuous cycle. In the case of satisfying a regulatory requirement, the initial stage of "Dissatisfaction" is created by the new legislation. That is to say, the new law causes the state of dissatisfaction if the organization is not already compliant with the new mandate. The second stage of "Search and Interact" is the organization's response to determine what modifications to the organization are required to meet the new mandate. The third stage of "Set / Envision Goals" is the process of defining the new business procedures to meet the new regulatory requirement. The final stage of "Implement Goals" is the execution of the business procedures defined in the previous stage. The rotation continues back to "Dissatisfaction" if the subsequent cycle did not produce an adequate change in the business to meet the mandated behavior or the results of the initial change causes a secondary state of dissatisfaction (see figure 1).

Research Method

A multiple case study methodology was selected to research the topic of this study because it is an appropriate method of research when "how" types of questions are being posed (Yin 2003). In addition, the research question of how Sarbanes-Oxley is impacting IT governance is relatively new and is not supported by a strong research base, providing more support for a case study approach (Benbasat, Goldstein and Mead 1987; Darke, Shanks and Broadbent 1998). Specifically, the study will be conducted as an explanatory multiple case study, with a positivist perspective. This approach allows the study to look for linkage between Sarbanes Oxley compliance and changes to IT governance (Yin 2003).

The research objectives of this study will be achieved through a field study that will examine three small to medium sized corporations. It will aim to follow the general qualitative case study guidelines put forth by Lincoln and Guba (1985) to extract the problem, the context, the issues, and the "lessons learned". More specifically, the embedded case study design will be used to facilitate examination of the primary impacts of the Sarbanes-Oxley Act on IT governance as well as any secondary effects the changes are having to IT governance.

The case study design is an appropriate research method for this study and for studies concerning information systems research for the following reasons:

1. It is an inquiry that allows a phenomenon (regulatory impact to IT governance) to be examined in a real life context (Benbasat, Goldstein et al. 1987; Yin 2003).
2. It focuses on a group of events and processes for which few studies have been done and in which we have no in-depth perspective (Benbasat, Goldstein et al. 1987; Creswell 1998).
3. It provides the ability to answer "how" and "why" questions which involves understanding the environment and complexity of the processes taking place (Benbasat, Goldstein et al. 1987).
4. It provides the ability to perform the investigation where the boundaries are not clearly evident (Hakim 1987; Yin 2003).

Expected Contribution

The expected contribution of this paper is a theory or model development that will better explain or predict the potential impact regulatory initiatives will have on IT governance. The development of such a model can then be used in broader studies to validate or refine the theories developed through this research. In addition, an IT governance regulatory impact model might be used by governing agencies to evaluate the potential changes a new law or standard might have on the organizations that will be bound by the new regulation. Further more, a specific organization might use this model to better understand and manage the changes a new regulation will have on its own IT department.

References

Benbasat, I., Goldstein, D.K., and Mead, M. The case research strategy in studies of information systems, *MIS Quarterly*, 11 (3), 369-386.

Bonham, S.S. *IT Project Portfolio Management* Artech House, Inc., Norwood, MA, 2005.

Broadbent, M., and Kitzis, E.S. *The New CIO Leader* Harvard Business School Press, Boston, MA, 2005.

Creswell, J. *Qualitative inquiry and research design: Choosing among five traditions* Sage Publications, Thousand Oaks, California, 1998.

Cule, P.E., and Robey, D. A Dual-Motor, Constructive Process Model of Organizational Transition, *Organization Studies*, 25 (2), 229-260.

Darke, P., Shanks, G., and Broadbent, M. Successfully completing case study research: combining rigour, relevance and pragmatism, *Information Systems Journal*, 8 (4), 273-289.

de Rond, M. On the Dialectics of Strategic Alliances, *Organization Science*, 15 (1), Jan/Feb 2004, 56-59.

Doz, Y.L. The Evolution of Cooperation in Strategic Alliances: initial conditions or learning processes?, *Strategic Management Journal*, 17 (Special Issue), Summer 1996, 55-83.

Hakim, C. *Research Design: Strategies and Choices in the Design of Social Research* Allen & Unwin, London, 1987.

Hooker, J.N. Is Design Theory Possible?, *Journal of Information Technology Theory and Application*, 6 (2), 73-83.

IT Governance Institute (2003) Board Briefing on IT Governance, 2nd Edition, www.itgi.org, accessed: 25 February 2005

Leih, M. (2006) IT Governance and the Sarbanes-Oxley Act, AMCIS 2006, August 4-6, 2006, Acapulco, Mexico,

Pare, G. Implementing Clinical Information Systems: A Multiple-Case Study within a US Hospital, *Health Services Management Research*, 15 (1), 71-92.

U.S. Congress (1996) The Clinger-Cohen Act of 1996. USC, 2/15/1996

U.S. Congress (2002) The Sarbanes-Oxley Act of 2002. House of Representatives 3763, USC, 23 January 2002

Van de Ven, A.H. Suggestions for Studying Strategy Process: A Research Note, *Strategic Management Journal*, 13 (Special Issue), Summer, 1992, 169-191.

Van de Ven, A.H., and Poole, S.M. Explaining Development and Change in Organizations, *Academy of Management. The Academy of Management Review*, 20 (3), 510-540.

Weill, P., and Ross, J. *IT governance: how top performers manage IT decision rights for superior results* Harvard Business School Publishing, Boston, 2004.

Yin, R.K. *Case Study Research: Design and Methods*, (3rd ed.) Sage Publications, Inc., Thousand Oaks, CA, 2003.