Governing Information Technology (IT) and Security Vulnerabilities: Empirical Study Applied on the Jordanian Industrial Companies

Asim El Sheikh, The Arab Academy for Banking & Financial Sciences, Jordan
Husam A. Abu Khadra, The Arab Academy for Banking & Financial Sciences, Jordan

ABSTRACT

The aims of this study is to evaluate information technology (IT) governance implementation using the COBiTs’ maturity model, investigate the perceived Security Threats that face these companies and measures the causality between them. An Empirical Survey using self-administered questionnaire has been carried out to achieve the study objectives. The study results reveal that Jordanian industrial companies did not apply IT governance in its comprehensive methodology despite the implementation of some of its aspects. The study main recommendation for the industrial companies that it should give more attention to IT governance. Industrial companies Professionals should work more to increase the IT governance strength for all of its dimensions especially with the existence of negative causality relation between the IT governance and security threats frequencies.

Keywords: Control; IT Governance; Maturity Model; Security; Security Threats

INTRODUCTION

Over the last decade, an evolution of auditing and IT security occurred as an irreversible movement toward the “electronization” of the business process. (Greenstein and Vasarhelyi, 2000). As a result many efforts herein
appeared as increasing interest to evolve the audit model toward a more action-driven method of control, revision and assurance, (Timothy et al, 1998). Several professional committees have undertaken this endeavor, such as the AICPA. However, these initiatives were in the form of general instructions, and nothing specific can be considered as detailed guidance to the auditors in their work. Accordingly, the responsibility has increased dramatically on the profession, to recognize and assess the threats which are associated with Control Systems (CS) in the IT environment. This partly due to the fact that technology in many cases developed faster than the advancement in CS, (Ryan & Bordoloi, 1997).

In addition, knowledge advancement in technology and related practices in the current age verify that the right practical employment is the key factor of technology and knowledge success (Oak Report, 2004). Enterprises realize that growing importance of information technology (IT) and consider it as a treasure enhancing their competitive position, adding value to their businesses. But what remains as a challenge is, which key practices that organizations should apply to get IT under control in order to deliver that desirable value? In other words what should be done govern IT activities? (Li et. al., 2007).

The current study aims to find the characteristics of IT governance in the Jordanian environment by using a self-developed model that are suitable to the domestic environment characteristics since no one size fits all (Rau, 2004), then applying this model on a sample from the Jordanian industrial companies. In addition, this study aims to investigate the security threats and control vulnerabilities that face the industrial companies. To date, little experience-based research have been conducted in Jordan and internationally to investigate security threats and what IT governance arrangement work best (Weill and Ross,A, 2004), where devising IT governance arrangements is challenging because the success of IT strategies and procedures is contingent upon a variety of internal and external factors (Bowen et. al., 2007).

RESEARCH BACKGROUND

Here below the theoretical discussion is split into two main sections, IT governance and Security Threats.

First Section: IT Governance

For many organizations, IT and IT infrastructure that constitute major investments, if not managed properly, may impair and incur losses rather than enhance the organization’s competitive position, on other words, organizations with effective IT governance have profits that are higher than other companies pursuing similar strategies. Moreover, the lack of effective IT governance has been shown to have adverse impacts on organizations, such as business losses, bad reputation, ‘runaway projects’, and