https://doi.org/10.48009/2_iis_2009_33-39

TOWARDS A FRAMEWORK FOR INFORMATION TECHNOLOGY GOVERNANCE IN PUERTO RICO

Sandra Fonseca Lind, Universidad del Turabo, Gurabo, PR, sandraflind@gmail.com
Mysore Ramaswamy, Southern University, Baton Rouge, LA, mysore@acm.org
Eulalia Márquez Martinez, Universidad del Turabo, Gurabo, PR, emarquez@suagm.edu

ABSTRACT

Everybody in today's highly networked corporate world is aware of the need for information security, since information is undeniably among an enterprise's most valuable assets. Therefore having a sound protection and data integrity infrastructure is paramount for corporate survival. In Puerto Rico, there are no regulations or formal standards regarding Information Technology (IT) governance for government agencies or small companies. Only companies which have their headquarters in the continental U.S., banking and pharmaceutical industries that are required to comply with Sarbanes Oxley (SOX) regulations are enforcing relevant control management models. Even though SOX compliance at first may seem to be an accounting and auditing matter, IT is at the heart of the issue. This is because the accuracy of financial reports relies in large part on decisions made by IT professionals. In this paper, we develop a framework for information technology governance even in organizations that are not specifically required to comply with SOX in Puerto Rico.

Keywords: Sarbanes Oxley, Information Technology Governance, Puerto Rico, Information Systems Controls.

INTRODUCTION

In Puerto Rico, there are no regulations or formal standards regarding information technology (IT) governance for government agencies or small companies. Armour [2] states that "human resource constraints, tight budgets, and the importance of doing more with less continually challenge departments of modest size." Only companies that have their headquarters in the continental U.S., banking and pharmaceutical industries that are required to comply with Sarbanes-Oxley regulations are enforcing their control management protocols. These control mechanisms come from headquarters in the form of a checklist with no provisions or flexibility for change. And still, no local control reporting structure or procedures exist to ensure the quality of operations is in place, providing grounds for fraud, embezzlement and other type of white-collar crimes. Small businesses and government agencies lack alternative controls establishment, management and compliance rules or regulations. Some guidelines have been established by the Office of Budget, Planning and Management in 1996 and updated in 2004. Agencies are unaware of the existence of these documents, or haven't done anything to follow them, since no rule or law actually requires compliance like Sarbanes Oxley does to US major corporations. The Puerto Rico Office of the Comptroller, Office of Government Ethics, the Financial Institutions Commissioner's Office and the Insurance Commissioner's Office are among local agencies in charge of performing all major audit to the agencies and to local small business, public corporations and government agencies in general. All of them have attempted to establish controls to be followed both operational and technological, but none of them has been successful in establishing a global standard in Puerto Rico. Therefore, no compliance enforcements standards alternatives, like the Sarbanes-Oxley Sections 302 and 404 applicable by law to small business, public corporations and government agencies are currently in place.

The Puerto Rico Government had tried on various occasions to centralize its Information Systems. Even now there is a Legislative Project presented at the Puerto Rico Senate called "Ley de Gobierno Electrónico" (Electronic Government Law: Information Knowledge Project) Project of the Senate – Law Number 151 of June 22, 2004. But as in the past, political issues have prevented these projects to become a reality, even though the need for document retention and storage regulation is extremely needed for audit and investigation purposes. Law 151 establishes public policy for the government of Puerto Rico in the process of adding electronic functionality to the operations of all Puerto Rico Government dependencies in order to transform the government to a digital one. The law also designates the Office of Management and Budget as the office in charge of managing all government agencies' information systems from technological requirements to standards and procedures relative to the proper use of electronic equipment and performs the assessment and development of all electronic transactions. The rest of this paper is organized as follows. First we discuss some salient points of SOX legislation. Then we propose a set of recommendations for IT governance suitable for businesses in Puerto Rico that are- not mandated to abide by SOX. Concluding remarks form the last section.

SARBANES OXLEY CONCEPTS

The Sarbanes Oxley Act of 2002 – signed by the President of the United States, George W. Bush on July 30, 2002 is a legislation passed in response to the accounting scandals with the purpose of assigning responsibilities to all those in charge of financial decisions within each company or corporation, and reinstate investors' trust and confidence in U.S. Corporations. These responsibilities range from accounting procedures, retirement funds management, and management controls. It also sets requirements for the management of Information Systems standards and procedures, applications parameters and processes, to assure general accepted accounting standards, as well as ensure that IT, financial and audit practices that are being followed. It also stipulates fines and consequences should the business not comply with the regulations stated in the bill. By doing this, not only investors and general public are protected against white collar fraud, but also the benefits and well-being of the employees of those companies is also protected. Compliance with this act will be administered by the Security Exchange Commission (SEC).

Ingram, Albright, et al [12] argue that "the failure of Enron Corporation's management to properly account for and report its business activities resulted in an understatement of the company's liabilities and an overstatement of profits." When the company's bad accounting practices became apparent in October 2001, creditors were unwilling to lend additional money to the company and investors tried to dump their stock. The value of Enron's stock dropped rapidly, and many of Enron's stock holders were employees of the company who had invested in the company's stock as part of their retirement plans. Many employees lost their jobs and their retirement savings as a result of these highly unethical events. These corporate fraud cases and the lines of defense followed by those indicted in the Enron Corporation trial (Kenneth Lay and Jeffrey Skillings), that they didn't know what was happening in the subsidiaries and they could not assure or certify the correctness of the corporation's financial statements, has been thoroughly analyzed not only from the accounting, audit and IT perspectives, but also being analyzed from an ethical point of view [17]. To this we might add the fact that until that time (2001), accounting laws were very old (1933-1940), and were enacted when the accounting and audit processes as well as the corporate process itself was completely manual and computers did not exist at the corporate level. The principal accounting laws passed before Sarbanes Oxley were 1) The Securities Act of 1933, 2) The Securities Exchange Act of 1934, 3) The Public Utility Holding Company Act of 1935, 4) The Trust Indenture Act of 1939, 5) The Investment Company Act of 1940, 6) The Investment Advisers Act of 1940, and 7) The Securities Investor Protection Act of 1970.

The defense strategy followed by Lay and Skillings provided the grounds for the Section 302 of the SOX act that requires that the principal executives officers (CEO and CFO) certify in each annual or quarterly report filed or submitted that:

1. They have reviewed the report and certify that the statement is true and correct.
2. They are responsible for establishing and maintaining controls.
3. They have designed, evaluated and presented internal controls and proved to be effective.

Section 404 of Sarbanes Oxley called "Management Assessment of Internal Controls" mandates that corporate CEOs implement internal controls over their financial reporting systems, physically test these controls, and certify in writing that they function correctly. In addition, the management must make sure that internal controls are adequately established and maintained and there is adequate internal control structure and procedures for financial reporting and an assessment is performed at the end of the fiscal year to evaluate the effectiveness of the control structure. It specifically states "The reporting must state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting" [8, 13].

The problem faced by information technology departments is the lack of directions in complying with the Act. Section 404 addresses the requirements of effective internal controls regarding financial statement reporting being in place, and the external auditors attesting that the management statement stating the existence of the controls is correct [2, 4, 19].

Due to Sarbanes Oxley reporting requirements and storage time requirements, Information Systems Department needs to act in order to be able to assure that all reports generated from their applications, both acquired and customized as well as in-house developed have all the necessary validations and selection criteria included in its code, processing steps are correct and the information will be securely stored for the five years required by it. This way reporting will be transparent and compliance will be possible. Accordingly, at the simplest level, the principal accountability of the CIO is to ensure that every step of a company's business process is documented and audited, and that all systems are in agreement and enforcing appropriate internal controls [1, 5, 7, 14].

According to Kinicki, Kreitner [16], "ethics" involves the study of moral issues and choices. It is concerned with right versus wrong, good versus bad and the many shades of gray in supposedly black-and-white issues. Moral implications spring from virtually every decision, both on and off the job." Compliance involves maintaining equity and ethics in every standard, policy or procedure. . Managers are challenged to evaluate every possible scenario and establish statutes to assure that both controls and employees rights and well-being are being covered.

Some industry analysts say that may be the Sarbanes-Oxley Act was released too early, but as Berghel [3] says "SOX was the congressional response to the corporate and accounting scandals that span the 15-year interval between the Solomon Brothers bond-trading scandal and the Enron and MCI-Worldcom incidents. Congress is making a definite statement with SOX: the "sleight-of-hand earnings" accounting philosophy that crept into U.S. business and the excuse "I just can't recall" won't cut it anymore". The unethical white collar behavior in these cases was huge, to the extent that the company is listed as the major corporate bankruptcy case in U.S. history. The Sarbanes Oxley Act of 2002 – signed by the President of the United States, George W. Bush on July 30, 2002 is a legislation passed in response to the accounting scandals with the purpose of assigning responsibilities to all those in charge of financial decisions within each company or corporation, and reinstate investors' trust and confidence in U.S. Corporations. These responsibilities range from accounting procedures, retirement funds management, and management controls. It also sets requirements for the management of Information Systems standards and procedures, applications parameters and processes, to assure general accepted accounting standards, as well as ensure that IT, financial and audit practices that are being followed. It also stipulates fines and consequences should the business not comply with the regulations stated in the bill. By doing this, not only investors and general public are protected against white collar fraud, but also the benefits and well-being of the employees of those companies is also protected. Compliance with this act will be administered by the Security Exchange Commission [9, 10, 11].

A FRAMEWORK FOR BETER REPORTING COMPLIANCE

Sarbanes-Oxley has become a very much needed piece of legislation for the enterprise community, for what was until then considered best accounting practices is now required by law and by being regulated, stockholder can invest with greater confidence. By establishing minimal requirements in terms of internal controls, both in operations and information systems applications and assigning accountability, the clarity of operations can now be enforced, resulting in having a solid platform for corporate investment. Ground for what will be considered corporate whistle blowing and information leaking must be depicted in corporate policy.

This does not restrain only to the United States. Japan, also faced some public companies financial scandals such as the Seibo Railway Case of October, 2004 and Live Door Co. Ltd., on January, 2007, known as the Japan's Enron. These two cases led to the passing of the "Internal Control Report System of the Financial Instruments and Exchange Law". It is called J-Sox even thou according to Shinji Hatta, Cahirman of Japan's ACFE Advisory Committee (2007) the "framework is not a copy of the US Sarbanes-Oxley Act". Hatta as cited by Carozza [6] defines the act as a "broad framework encompassing all the efforts to improve confidence in the Japanese listed companies. Special attention in the framework is given to the internal control provision of Section 404 of the US Sarbanes Oxley Act because it has affected U.S. public companies more than any other section in the legislation". This could be caused by the fact that almost all corporate operations depend completely in IT applications.

The importance of accurate reporting of financial information cannot be overemphasized. Even though Sarbanes Oxley compliance at first may seem to be an accounting and auditing matter, information technology (IT) is at the heart of the issue. This is because the accuracy of financial reports relies in large part on decisions made by IT professionals. While CEOs and CFOs sign their names to legal certifications in the annual report, an increasing number of companies are also requiring their Chief Information Officers to sign a "sub-certification," regarding the controls, processes and overall accuracy of the IT assets they manage. Organizations which fell under the mandatory SOX compliance requirement are now looking back at the substantial investments in time, effort, and money that were made in order to meet the regulatory requirements. These companies are also looking for ways to automate and simplify processes to alleviate some of the compliance risks and associated costs. In this context, the need for a compliance framework that is not too cumbersome as to be shunned by businesses has to be developed for the consideration of businesses in Puerto Rico which are not mandated to have SOX compliance. In this section, we take a fresh look at the issue of information technology governance, and give recommendations that are less convoluted and more effective.

According to Kaarst-Brown and Kelley [14], SOX targets both management accountability and operating efficiencies as indicated in Appendix I. They also conclude that more studies must be made on the impact of SOX compliance as an opportunity of studying organizational transformation, information systems integration and IT functional adaptation. The principal accountability of the CIO is to ensure that every step of a company's business is documented and audited, and that all systems are in agreement and enforcing appropriate internal controls. The impact of information systems and processes are numerous. They include reporting content, timeliness, retention and destruction policy, detailed documentation, and integration of information from manual and automated processes.

According to Turban and McLean [20] information system collects, processes, analyzes and disseminates information for a specific purpose. An information system includes inputs (data, instructions), and outputs (reports, calculations). It processes the inputs and produces outputs that are sent to the users or to other systems as indicated in Appendix II. A feedback mechanism that controls the operation may be included. Like any other system, and information system operates within an environment. An information system can be formal or informal. Formal systems include standards, procedures, standard inputs and outputs and fixed definitions [15].

CIO Insight and Gartner polled 198 firms of various sizes and industries to find out what they felt was their biggest obstacle in getting their IT organization compliant, the top four reasons were the following:

(1) How data is now structured in their systems,
(2) Insuring adequate security and business continuity,
(3) Inadequate IT budget, and
(4) Variations in infrastructure between business units and subsidiaries.

Even though there are some IT control guidelines established by the Puerto Rico Government back in 1996 and revised in 2004 called Operational IT Guidelines (Guias Operacionales) , and also a piece of legislation, Law # 151 of 2004, Electronic Government, still Puerto Rico lacks the awareness of proper corporate accounting management and IT control structure. Cases like Enron, Worldcom, Tyco and even the Department of Defense are viewed as remote incidents that haven't happened locally and probably never will.

This managerial way of thinking poses a risk to the IT and general business and entire business as well as government environment, since controls compliance do not have a high priority. Consistency in applications is neglected, resulting in numerous findings in diverse audits to government agencies IT divisions.

The Puerto Rico Office of the Comptroller has a division dedicated to audit the Information Systems Departments of all Puerto Rico's Government agencies IT Departments in order to assure compliance with laws and regulations, and to make sure all best administration practices are applied. For our study, a survey was made by evaluating all the published reports from the year 2001-2002 thru 2006-2007 and all related findings to the study were classified as follows:

(a) Findings related to deficiencies in network controls.
(b) Findings related to absence in network controls.
(c) Findings related to deficiencies in access controls.
(d) Findings related to absence in access controls.
(e) Findings related to deficiencies in standards and procedures.
(f) Findings related to absence of standards and procedures.
(g) Findings related to deficiencies in application controls.

(h) Findings related to absence in application controls.
(i) Findings related to deficiencies in user awareness.

From a preliminary analysis of the above survey, we observe that the following areas are of concern:

(i) Absence of standards and procedures,
(ii) Multiple agencies causing redundancy,
(iii) Deficiencies in application controls, and
(iv) Deficiencies in network controls.

Based on the above, we can identify the factors to improve IT governance based on the four stages referred to in Appendix II. The input stage is critical in ensuring accuracy of reporting. Sometimes, CIOs are called "stewards of data accuracy" [12]. At this stage, input controls and business rules have to be clearly defined and documented. In order to process the input data, the criteria spelt out for controls regarding authorization, authentication, validation, and verification have to be stringently adhered. Processing is by far the most critical stage where people, processes, and technology interact. The output stage has to be designed to ensure proper reporting as well as to provide testing and storage capabilities.

Compliance can be viewed as establishing the programs or processes designed for the purpose of evaluation and which ensure that all departments and personnel are aware and follow all rules, standards and regulations that are in place in the corporation. It is necessary that the IT security personnel be involved from the very beginning – system analysis and development stage – so that necessary security safeguards can be properly built into the system. Top management support is essential so that adequate resources are at the disposal of the CIO. The standards play an important role and it has to be ensured that all business units and subsidiaries have the same infrastructure. To summarize, the recommendations for optimal IT compliance are as follows:

(a) Involve IT security personnel from the very beginning,
(b) Ensure strict data quality standards,
(c) Design optimal process flow,
(d) Obtain support from top management,
(e) Adhere strictly to standards and regulations, and
(f) Evaluate the performance periodically and make necessary corrections.

CONCLUSION

Sarbanes Oxley regulations have once again shown the importance of accurate financial information reporting. Even those businesses that are not mandated to abide by SOX regulations, realize the importance of proper IT compliance. The role of Information Systems Security Professional in Puerto Rico is still not clearly understood, and most of the times they are held responsible for evaluating and assuring that systems and application controls are in place. In this paper, we have reviewed the salient aspects of Sarbanes Oxley regulations. We have also viewed the compliance issue from an IS perspective. The recommendations given here are intended to assure accurate reporting of financial information based on sound system design that includes inputs from IT security personnel from the very beginning.

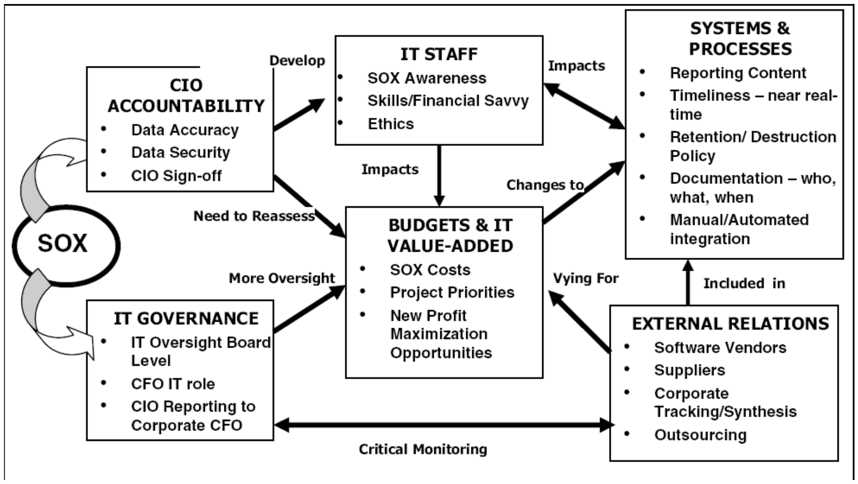
REFERENCES

1. Al-Mashari, Majed, Zahir Irani, & Mohamed Zairi. (2001). *Business process reengineering: a survey of international experience*. *Business Process Management Journal*, December 2001, pp. 437-455.

2. Armour, Phillip G. (2005). *The Business of Software – Sarbanes Oxley and Software Projects.* Communications of the ACM. 48.6.p.15-17.
3. Berghel. Hal. (2005). *The Two Sides of ROI. Return on Investment Vs. Risk of Incarceration.* Communications of th ACM. 48.4. p15-20.
4. Bisoux, Tricia. (2005). *The Sarbanes Oxley Effect.* BizEd. July/August. Retrieved on May 2, 2007 from URL:www.aacsb.edu/ publications/JulyAug05/p24-29.pdf
5. Busta, Bruce. Portz, Kris. Strong, Joel. Lewis, Roger. (2006). *Expert Consensus on the top IT Controls for a Small Business.* Information Systems Control Journal. Vol. 6, 2006 pp.22-23.
6 Carozza, Dick. (2007). *Japan Works to Deter Fraud with J-Sox.* Fraud Magazine. 21:6 pp37-43
7. Grimaila, Michael, R. Kulkarni, Abhijit, S. (2005). *Challenges is Achieving Sabanes-Oxley Compliance.* The ISSA Journal. February, 2005.
8. Hall, James A. Liedtka, Stephen L. (2007). *The Sarbanes Oxley Act: Implications for Large-Scale Outsourcing.* Communications of the ACM. 50.3.

9. Herrod, Chrisan. (2006). *The Role of Information Security and Its Relationship to Information Technology Risk.* Reading from Readings and Cases in the Management of Information Security. Thomson Course Technology. Canada.
10. Hilton, Ronald W. Maher, Michael W. Seltho, Frank H. (2006). *Cost Management – Strategies for Business Decisions*. 3rd. Ed. Irwin, McGraw Hill, New York, 2006.
11. Hunton, J.E., Bryant, S. M. & Bagranoff, N. A. (2004). *Core Concepts of Information Technology Auditing*. Wiley Publishing. New Jersey.
12. Ingram, Robert W. Albright, Thomas L. Baldwin, Bruce A. Hill, John, W. (2005). *Accounting – Information for Decisions.* Thomson South Western, Canada.
13. IT Governance Institute (ITGI). (2004). *IT Control Objectives for Sarbanes Oxley, The Importance of IT in the Design, Implementation and Sustainability of Internal Controls over Disclosure and Financial Reporting.* IT Governance Institute.
14. Kaarst-Brown, Michelle L. Kelly, Shirley. (2005). *IT Governance and Sarbanes-Oxley: The latest pitch or real challenges for the IT Function?* Proceedings of the 38th. Hawaii International Conference on System Sciences.
15. Kendall, K. E. & Kendall, J. E., (2002), *System Analysis and Design,* 5th Ed., Prentice Hall.
16. Kinicki, Angelo. Kreitneer, Robert. (2006). *Organizational Behavior – Key Concepts, Skills and Best Practices.* 2nd. Ed. Irwin, McGraw Hill. New York
17. McLarney, Carolan. Dastrala, Ramakrishna. (2001). *Socio-Political Structures as Determinants of Global Success – The Case of Enron Corporation.* International Journal of Social Economics. 28.4.pp.349-367.
18. Peltier, Thomas R. (2002). *Information Security Polices, Procedures and Standards – Guidelines for Effective Information Security Management.* Auerbach Publications. Florida.
19. Stephens, David O. (2005). *The Sarbanes-Oxley Act – Records Management Implications.* Records Management Journal. 25, 2, 2005. pp.98-103.
20. Turban, Ephraim. McLean, James. (2002). *Information Technology for Management – Transforming Business in the Digital Economy.* 3rd. Ed. John Wiley & Sons.

Appendix I. The IT Compliance and Controls Dilemma (Adapted from [14])



Appendix II. Process Control Flow