https://doi.org/10.48009/1_iis_2014_224-234

Issues in Information Systems
Volume 15, Issue I, pp. 224-234, 2014

INFORMATION TECHNOLOGY ARCHITECTURE FOR OPTIMAL REPORTING

Sandra Fonseca-Lind, Universidad Metropolitana, San Juan, PR, sfonseca3@suagm.edu
Mysore Ramaswamy, Southern University, Baton Rouge, LA, mysore@acm.org

ABSTRACT

In today's highly networked corporate world, information is undeniably among enterprise's most valuable assets. Information Technology (IT) has taken the additional responsibilities for business support and report generation. The 'new' economy has given way to 'now' economy or real-time economy. This has resulted in a substantive acceleration of business measurement, assessment, reporting, and decision making processes. To what level the compliance evaluation programs must be implemented in the company, or government agency to assure precision, quality, efficiency, and effectiveness of operations needs to be analyzed. Too often, the system designers and/or the packaged systems focus on the financial reporting output to the neglect of the internal reporting needs. Even though Sarbanes-Oxley (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 analyze some of the factors that are critical to compliance and reporting issues and propose a set of recommendations which in addition to compliance, can pave the way for better business reporting.

Keywords: Information Technology Controls, Information Technology Governance, Sarbanes-Oxley Compliance, Real Time Economy.

INTRODUCTION

Information technology (IT) controls have become very critical in today's information systems infrastructure as it affects the operations of all businesses and government agencies. IT has taken the additional responsibilities for business support and report generation. Due to their strategic nature within companies, information technology projects and information management are now complex and have higher budgets, schedules and associated risks. Everyone is aware of the importance of information security management in the current web-based highly networked business environment. What is still unclear is to what level the compliance evaluation programs must be implemented in the company, or government agency to assure precision, quality, efficiency, and effectiveness of operations. At the higher management level, the Chief Financial Officer (CFO) still views the Chief Information Officer (CIO) more operational than strategic in nature.

As organizations are becoming more and more dependent on technology for conducting its business, the pressures on the IT function are higher. The requirements to provide fast results for the operations of the company are constantly increasing. Many a times, this results in the quality of operational performance and IT controls becoming less important compared to the operational speed and the ability to quickly adapt to market tendencies. The management seems oblivious to the risks and threats. The use of IT as part of an organization's strategy for competitive advantage or even survival is badly mishandled by complexity and high cost [3, 10]. Despite cases of successful IT development projects, it is widely accepted in the field that an unacceptable number of projects will fail.

There is a gap between IT controls and effectiveness that causes businesses to loose revenue and customers every year not to mention the decrease in productivity and the precision of the operations. Technological change has always catalyzed organizational change thus having an impact on IT controls and overall governance. The rest of this paper is organized as follows. First we look at some salient points of Sarbanes Oxley Act. Then we explore the ways to restructure financial/managerial reports. Finally we propose a set of recommendations for IT governance that takes a holistic approach.

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. The Security Exchange Commission (SEC) will administer compliance with this act.

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 stockholders 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 facts 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 were 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 employee's 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].

RESTRUCTURING OF FINANCIAL/MANAGERIAL REPORTS

If all internal and external stakeholders in the firm shared the same information about how the firm has performed in the past and had similar expectations as how it will perform in the future, financial reporting would not be all that critical. Such an ideal situation does not exist, and those within the firm are inevitably in a better position to know its state than those stakeholders outside of it [27]. The internal stakeholders have a significant information advantage if the internal reporting system has been set up properly**.** Herein lays the fundamental informational asymmetry. Shareholders only care about the financial performance of the firm as reflected in the market price. Managers' main concern would be the optimal way to leverage the assets of the company. Other stakeholders in the company such as employees, creditors, suppliers, customers, and local agencies have their own interests and look to managerial accounting reports rather than financial statements to obtain relevant information that will help in their decision making.

Based on the analysis conducted by Vasarhelyi [28], in order to render an authentic mapping, the following questions need to be asked:

- Should accountants measure levels for the balance sheet of items that are elements in the value chain but not belonging to the entity, such as supplier managed inventories?

- Do they need to measure the levels at the partners that supply this inventory?
- Do accountants need to consolidate these values along the value chain to represent the situation of the value chain?
- Within the framework of the Numerical Representational System, are there factors to be measured that are not numerical, such as flow of information about the company, patents, ethical tone, etc.?
- Are the rules of valuation linking the two systems constant or variable depending on contingencies?
- Should the systemic risks and element specific risks be disclosed?
- Should the assumed relationships of business elements and the ensuing operational business models be disclosed?

Enterprise Resource Planning (ERP) systems are successful in achieving efficiencies in supply chain management. However, the same cannot be said regarding the mapping of business transactions into financial reports using modules such as SAP Financial Accounting modules. In order to ensure an accurate mapping of transactions, it is essential that accuracy has to be assured at the following levels: Process Level, Data Level, and Opinion Level. At the Process Level, all processes internal and outsourced need to be monitored, consolidated, and the output of this level feeds into the next level, Data Level. Here all the data is verified and the output feed to the next level, Opinion Level where reports are generated. Methods of continuous assurance have to be developed for all three of these levels in order to properly monitor the reporting of transactions in this digital age. The success of digital accounting will depend on the following factors: (a) Incorporating filters that limit direct takeover in the accounting database from in and out of the enterprise, without the prior verification by the specialized staff, and (b) The manner in which the specialized staff process the data in their database simultaneously with the data already processed by other subsystems.

To make the information produced and provided in the electronic accounting information system more reliable, electronic accounting principles were developed by the International Federation of Accountants (IFAC). These principles can be broadly classified as Security Principles and Process Principles. Figure 3 displays the preferred quality characteristics of an Accounting Information System (AIS). Based on the definition of the International Organization for Standardization, quality is a group of features and characteristics of product, process, or services that are relative to a set of requirements that will result in user satisfaction. If those inherent characteristics meet all requirements, high or excellent quality is achieved. If those characteristics do not meet all requirements, a low or poor quality is achieved. To enhance quality, it is necessary to minimize or eliminate those activities that do not add value to business entity. The quality of AIS depends on input quality, data processing quality, and output quality.

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.

Enterprise Resource Planning (ERP) packages are complex information systems capable of supporting all functional areas of an enterprise corporation or government agency or even academic/non-profit institution. ERP usually improves and speeds business operations because of its proposed integrated modular structure. But by being complex in nature its implementation and maintenance is difficult and costly. One of the objectives for Service Oriented Architecture (SOA) framework process modeling is to provide a centralized and consistent model for application modeling, controls establishment, implementation and assurance, as well as risk management, scalability and compliance assurance. This provides a proper framework capable

of effectively combining regulations, proper operational processes, content management, usability of having a repository of printed reports available on electronic format and security.

As Weerakkody, Bare & Choudrie [26] state "given the nature of the diverse that span government information technology infrastructures, the emerging concept of web services cannot be ignored. Web services promises to offer a solution to the Enterprise Application Integration (EAI) problem through the use of Business Process Management (BPM) and Service Oriented Architecture (SOA), where large service providers are working together to develop a common platform and standard for modern EAI". Implementing and keeping in place some of the proper Information System controls is not an easy task. In Puerto Rico it is not an exception that 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, and like the Project Manager, this task must be accomplished without any control or participation during the early stages of application development. Systems Security Professionals are usually the last to know about an upcoming audit, but are the first to take the heat or the blame when a finding occurs or something goes wrong in IT.

Unfortunately, Puerto Rico's government do not see itself as a potential fraud or hacking scheme target because nothing huge such as Enron, WorldCom or the other scandals have not happened to them yet. But there are a lot of flaws and security holes from systems to applications to systems setting, to controls and compliance programs. Upon an informal research performed among various Systems Security Professionals from the Puerto Rico government agencies about their systems security standards, controls and compliance management, and even though many of them have someone appointed to security duties, all of them are still very limited. Some even believe that systems security consists mainly on controlling email and Internet access security (firewall administration). But very few of them are aware of the legal impact of the job of a Systems Security Professional.

When standards, procedures, and controls are established, the evaluation of the economic and legal impact of later compliance must be carefully evaluated. Sometimes this fact is overlooked or vaguely evaluated, which could lead to management's concern over certifying IT controls they are not completely sure are correct, precise and therefore effective. The oversight and internal controls problems can and will affect the accuracy and thus reliability of financial reports [11]. Through the years and multiple application projects developed and implemented both in small companies and agencies as well, failure to set and maintain a proper control measurement and IT quality assurance program, the task of keeping security holes and application inconsistencies becomes complex and even unable to keep. To this we might add the political issue. Every four to eight years the government shifts from political party control, with the immediate effect of projects being delayed or even cancelled. While most of the IT related projects are contracted within the government period, there are no grounds for IT projects to be kept even though professionals linked to previous administrations, leading to constant failures in government, designed them.

Through the main Project Management phases, requirements and testing are mentioned but sometimes vaguely and given lower priority should the project fall behind schedule or go over-budget. A proper security mapping structure to be followed in IT applications development projects has not been properly established, and this could be caused by the uncertainty regarding the role of security in Information Technology. This study intends to identify the activities needed to enforce security and compliance in project management, application maintenance, and overall IT policy and reporting structure and present a framework for control establishment assurance during IT application development projects.

By specifically mapping security in the application development and implementation process, the main vehicle for providing the necessary validations and selection criteria included in its code and parameter settings, the probability of correctness of the processing steps will be higher, risk will be properly controlled and mitigated, and the information will be processed and stored. This becomes a critical issue in an era of portable computing and scalability, such as Portals, Service Oriented Architecture and enterprise computing. With the proposed compliance model for information systems, that could be useful for both government agencies and municipalities of Puerto Rico, management controls risk management and proper reporting standards could be now transparent and an achievable goal. Information Systems

Departments need to act in order to be able to make sure all reports generated from their applications, both acquired and customized as well as in-house developed have 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 that currently is being considered as a best practice for record and information keeping. This way reporting will be transparent and compliance will be possible at the time of internal or external audits. 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. [14, 17]

CONCLUSIONS

The Information Technology Management Reform Act of 1996 (Clinger-Cohen Act) the law demanded that federal agencies follow corporate America's best practices for managing Information Technology. Agencies were required to hire a Chief Information Officer (CIO), institute investment controls and establish performance goals and metrics to measure success. The law was hailed as the tool that would finally fix federal IT. It was thought as the much-needed measure to change the way government looked at Information Technology (IT), but nothing really has changed. The main objective behind this piece of legislation was to turn the CIO from the technology person that fixes things or do strange things in the computer systems to be a strategic player within the company, institution or agency. It fell short to political interests. This is one reason why Information Governance (IT) has become paramount for any enterprise to be successful and competitive. Laws need to have compliance enforcement mechanisms in order to be effective like SOX and HIPAA. Also laws need to empower the CIO to be successful and effective. The CIO's views in the government need to change. According to former CIO of DHS, Steve Cooper, "in most of the departments where the CIO does not report to the secretary, the CIO is marginalized. Since CIO's are process and solutions oriented, many times their points of view slashes with the Chief Information Security Officer's (CISO's) points of view of ensuring first that the solution is viable and secure; CISO's must not report to the CIO, because they will also be marginalized. CIOs should not be seen as those who fixe PCs, laptops, blackberries, make the printer work, or make PowerPoint presentations or Excel spreadsheets. CISOs should not be viewed only as paper-checkers, firewall or anti-virus administrators but strategists as well.

Highly trained, technical and managerial people must direct today's complex IT projects. Twice in a period of three years, the Transportation Security Administration abandoned the CAPPS II airline passenger screening system over delays, over-budget and security/privacy concerns raised. Its replacement project, The Secure Flight Project also faced privacy concerns and technical issues because of a lack of a clear project-management plan. One lesson government hasn't learned and the best run businesses have is to fail fast. The inertia of long government budget cycles can lead to good money chasing bad projects, whereas business might put a halt to a failing program faster than government, because the private sector cuts off failures before they become failures.

The government budget cycle is a problem that isn't going to change, any more than IT leader at publicly traded companies are going to get a break from the pressure of quarterly earnings targets. But there are other areas where people and process changes can make a difference. In the case of the FBI Virtual Case File System project failure, over a 3-year run, five (5) CIO's and nine (9) program managers passed through it. This is fatal for any project, IT-oriented or not. Many agencies haven't developed processes, or the latest pipeline to get the skilled managers on the projects that need them. One reason project management is so critical is the degree to which government leans on contractors. Also processes must be carefully evaluated. That is one of the main reasons why legislation like Sarbanes-Oxley has become the ad-hoc standard for financial transparency, trust and corporate accountability. While mandatory for all publicly-owned companies, Sarbanes-Oxley is also becoming a best practice for all types for companies who wish to identify with good governance practices. A significant amount of attention is currently focused on Section 302 (Disclosure) and 404 (Internal Controls). Sarbanes-Oxley Sections 302 and 404 are designed to ensure information required to be disclosed is initiated, processed, recorded and reported and that management has assessed the effectiveness of internal controls regarding the reliability of financial

reporting. This constitutes the spinal cord of Information Governance (IT) and Corporate Governance as well.

Congress passed the Clinger-Cohen Act of 1996 to instill private-sector IT management best practices in federal agencies and required agencies to hire a CIO. The CIO was envisioned to be a top-level executive who would provide strategic insight into how IT could help mold the business processes used to deliver public services. The law also did away with much of the bureaucratic processes of thinking they were required to follow to purchase IT equipment, program and services which prolonged much procurement by years. The Clinger-Cohen Act's primary provisions are:

- Create a CIO position that reports to the head of the agency
- Develop an IT capital planning and investment process
- Sets performance goals and standards for IT systems
- Create an enterprise architecture
- Evaluate the skills of the agency's IT staff and identify skill gaps.
- Evaluate the IT skills of the agency's executives.
- Develop hiring and training plans for the agency's workforce to improve IT management.

Why it failed:

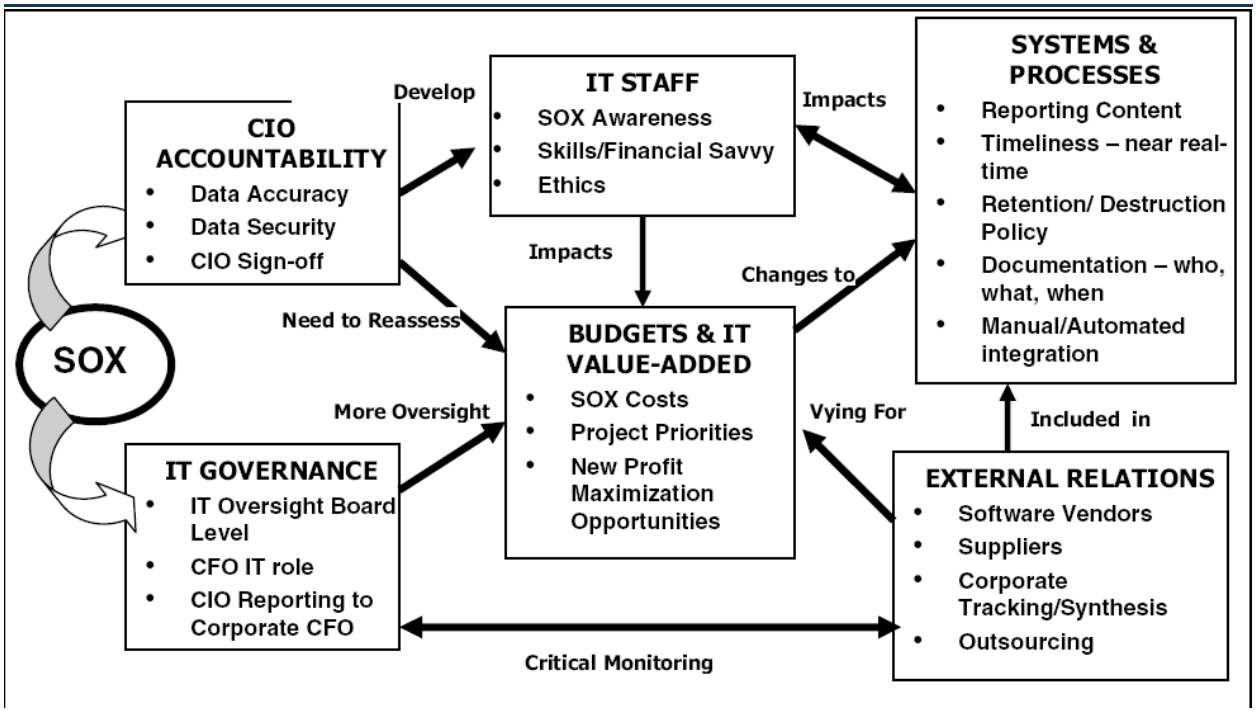
- Most federal CIO'S do not report to the head of the agency and few have full authority over the agency's IT budget.
- Capital planning and investment reviews are still seen as paperwork.
- Few agencies measure whether performance goals and standards have been met and are given little guidance on how to do so.
- Most agency architectures are too technical and detailed (down to the desktop) and do not serve as a blueprint of an agency's business processes, including where systems need to be interoperable and the best way to apply technology.
- Lack of Project Management Skills is still cited as one of the primary causes or project failure.
- Agency leaders still lacks knowledge of IT's role. Agency also lacks knowledge of the CISO's role.

Based on the above findings, we make the following recommendations. A viable Information Systems Audit Committee should be formed and scheduled to meet at least monthly. The CIO must have autonomy and a proper reporting control structure. All relevant service areas of the government must participate in it and then report the efforts of the committee not only to every agency higher management but also to the MIS and the IT personnel to ensure communication and awareness of the state of applications and general operations. Operations continuum must be enforced and protected through administration changes. The talent and knowledge of the existing personnel needs to be maximized. 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, especially for the government and small businesses IT operations.

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.pp. 15-17.
3. Bharati, Pratyush. Berg, Daniel. (2003). *Managing Information Systems for Service Quality – A Study from the Other Side. Information Technology & People Journal 16(2) 183-202*
4. Bassett, Jackie. (2007). *Security in Management's Terms.* Internal Auditor. *LXIV*:III. pp.27-31.
5. Berghel. Hal. (2005). *The Two Sides of ROI. Return on Investment Vs. Risk of Incarceration.* Communications of the ACM. 48.4. pp. 15-20.
6. Bisoux, Tricia. (2005). *The Sarbanes Oxley Effect.* BizEd. July/August. Retrieved on May 2, 2007 from URL:www.aacsb.edu/publications/Archives/JulyAug05/p24-29.pdf

7. 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, pp.22-23.
8. Champy, James. (2002). *X-Engineering the Corporation. The Next Frontier of Business Performance.* Warner Business Books. New York
9. Ciganek, Andrew P. (2006). *The Need for Speed. The Decision to Adopt Service-Oriented Architecture.* University of Milwaukee. Retrieved on June 30, 2007 from URL: http://proquest.umi.com/pqdweb?index=23&did=1232407811&SrchMode=1&sid=3&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1183517351&clientId=2606
10. Fonseca-Lind, S et al (2008), Indirect Consequences of Sarbanes Oxley on IT Governance in Puerto Rico, *IABPAD Proceedings*, pp. 528-538.
11. Goulielmos, Markos (2003). *Outlining Organizational Failure in Information Systems Development.* Disaster Prevention and Management Journal. 12:4. Pp319-327.
12. Hall, James A. Liedtka, Stephen L. (2007). *The Sarbanes Oxley Act: Implications for Large-Scale Outsourcing.* Communications of the ACM. 50.3.
13. 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.
14. Hertzberg, Robert. (2007). Top 10 IT Projects in 2007. Innovations Magazine Issue 4.
15. Hunton, J.E., Bryant, S. M. & Bagranoff, N. A. (2004). *Core Concepts of Information Technology Auditing*. Wiley Publishing. New Jersey.
16. Ingram, Robert W. Albright, Thomas L. Baldwin, Bruce A. Hill, John, W. (2005). *Accounting – Information for Decisions.* Thomson South Western, Canada.
17. 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.
18. 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.
19. Kendall, K. E. & Kendall, J. E., (2002), *System Analysis and Design,* 5th Ed., Prentice Hall.
20. 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.
21. Peltier, Thomas R. (2002). *Information Security Polices Procedures and Standards – Guidelines for Effective Information Security Management.* Auerbach Publications. Florida.
22. Robbins, Fred. (2006). *Corporate Governance after Sarbanes-Oxley: an Australian Perspective.* Corporate Governance Journal 6, 1, 2006 pp. 34-45.
23. Ross, Jeffrey. (2007). *Delivering Research: Impact to Business and Government.* E-Government Forum. Sydney.
24. Ross, Steven J. (2007). *Compliance and Beyond.* Information Systems Control Journal. 4 pp. 5.
25. Turban, Ephraim. McLean, James. (2002). *Information Technology for Management – Transforming Business in the Digital Economy.* 3rd. Ed. John Wiley & Sons.
26. Valacich, J. S., George, J.F., & Hoffer, J. A. (2001). *Essentials of Systems Analysis and Design. New Jersey:* Prentice Hall.
27. Weerakkody, Vishanth, Baire, Simon, & Choudrie, Jyoti. (2006). *E- Government: The Need for Effective Process Management in the Public Sector.* Proceedings of the 39th Hawaii International Conference on Systems Sciences. Hawaii.
28. Whitman, Michael E., & Mattord, Herbert J. (2004). *Management of Information Security.* Thomson Course Technology. Canada.



APPENDIX I

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