https://doi.org/10.48009/1_iis_2013_197-206

TOWARDS AN OPTIMAL ARCHITECTURE FOR INFORMATION TECHNOLOGY GOVERNANCE IN PUERTO RICO

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

ABSTRACT

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. This paper examines the reporting standards and controls in companies and government agencies in Puerto Rico, the impact of implementing such controls, measurement of their results, as well as their level of knowledge of the accuracy of the application controls that are implemented in their companies. The main objective of this study is to develop and propose a centralized governance and compliance standard for Information Technology Departments of both small agencies and government agencies in Puerto Rico, improving upon the current Law 151 and Office of Management and Budget Operational Guidelines established by Letter 77-05 dated December 8, 2004.

Keywords: Information Technology Controls, Information Technology Governance, Service Oriented Architecture, Puerto Rico

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, these 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 fail.

As Ciganek [9] states, "there is a need for an increased responsiveness to the external environment to attain or maintain competitiveness, the ability to capitalize on potential new markets, or simply a means to minimize costs, decision speed is both desirable and increasingly necessary for survival among organizations." But there is a gap between 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 discuss some salient points of IT Governance and IT Controls in Puerto Rico. Then we present the research methodology followed by an analysis of results. Finally we propose a set of recommendations for IT governance suitable for businesses in Puerto Rico.

IT GOVERNANCE AND COMPLIANCE ISSUES IN PUERTO RICO

In Puerto Rico, there are no regulations or formal standards required for the government agencies or small companies. Only companies that have their headquarters in the continental U.S., banking and pharmaceutical industries are required to comply with Sarbanes-Oxley regulations, are enforcing their control management models [6, 10]. These models come from headquarters in the form of a checklist with no provisions or flexibility for change. No local control reporting structure or procedures to ensure the quality of operations is in place, providing grounds for fraud, embezzlement and other type of white-collar crimes. Small business and government agencies lack an alternative controls establishment, management and compliance rules or regulations. The Office of Budget, Planning and Management in 1996 and updated in 2004 and 2007 have established some guidelines. Agencies are unaware of the existence of these documents, or have not 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 the 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 operationally and technologically, but none of them have 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 businesses, 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 absence of inter-system control mechanisms, consistent systems frameworks and the lack of auditable sources of data will make it very difficult to assert that the accounts are accurate. In this study, the reporting standards and controls by companies and government agencies in Puerto Rico were evaluated. In addition, the legal and economic impact of implementing such controls, measurement of their results, as well as their level of knowledge of the accuracy of the application controls that runs on their company's systems were also studied in order to develop a centralized governance and compliance standard model for Information Technology Departments of both small agencies and government agencies in Puerto Rico.

The Puerto Rico Government agencies face a lack of an IT Governance and Compliance standard requiring them to have in place a set of standards and procedures and enforce its proper maintenance. Should agencies have this set of standards properly stated, findings at Information Systems audits would be contained. Even though the Office of Management and Budget first published a set of guidelines aimed at establishing IT controls in the agencies in 1996 and revised them in 2004. Government agencies have not been consistent in its implementation and maintenance, resulting in a pattern of access and IT controls related findings. Also there is absence of application development/implementation project management standards to follow every time an IT project is executed. Efforts for E-Government and Infrastructure Standardization have failed.

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.

RESEARCH METHODOLOGY

The research questions for this study are stated below.

- What are the different levels of complexity involved in the various processes of reporting compliance under the current IT governance structure applicable to different organizations? Why hasn't the government established a centralized governance and compliance model and implemented it to be followed by all agencies and small companies?
- What controls and compliance requirements need to be established to make information processing effective and robust? What characteristics of authentication, verification and certification should applications have to provide a reliable reporting structure for management?

● How can a Security Professional establish and maintain an effective control and quality assurance program that is realistic and cost-effective to the company, agency or institution? What does he/she needs in order to be able to make systems security possible?
● What are the necessary steps an organization has to take to establish effective IT governance and control framework? What are the specific activities, deliverables and controls that must be incorporated to the project management model and systems development life cycle activities to make this objective achievable, especially in complex applications such as Enterprise Resource Planning (ERP)?

The main objective of this research is to propose a control assurance framework for application design for Project Management to ensure effective IT controls and compliance are achieved in organizations such as government agencies in Puerto Rico. The role of information security in IT application development will be included in the proposed framework, ensuring general IT controls as well as authenticity and integrity in operations. This way the IT function will be an efficient and effective one. The framework will be designed considering complex applications such as Enterprise Resource Planning (ERP) solutions and Service-Oriented Architecture (SOA). The above objective will be achieved by addressing the following secondary objectives:

1. Critically evaluate the current systems analysis and design as well as project management models with emphasis on IT controls and validation rules design.
2. Perform a comparative analysis of the current trends in Information Technology (IT) such as Enterprise Resource Planning (ERP) systems and Service Oriented Architecture (SOA) and revisit data modeling and control validations from the early stages of systems analysis.
3. Critically evaluate the current role of Systems Security within IT application implementation project management, design and propose a standard role on establishing and ensuring correctness and compliance on IT controls and validation rules design.

Some possible causes for systems and application flaws that could in some part contributed to the fraud cases reported recently, could reside in the project management scheduling activities models, where system security controls are being left to the testing and even implementation phases, when in fact, systems security must be present even from the pre-planning stages. Unfortunately, security is relegated for testing and implementation phase, which is essentially a reactive stage. Therefore the controls, validations and security measures are not taken as carefully and seriously as system security would have or like, making the compliance issue cumbersome. Should a complete code-walkthrough be performed within the system's development testing activities prior to accepting a project, parameter and code validation criteria could be certified and future concerns about the correctness of the results made practically nonexistent. Carefully planning and testing all validation criteria and configuration parameters within application development should make IT reporting and validation made transparent.

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]

RESULTS

According to Berghel [5] "Because electronic data processing is a staple of modern business and industry, provisions of SOX impose considerable responsibilities to the modern CIO. SOX makes the CIO's responsibility to put fraud detection systems in place, prevent inside compromises of the IT environment, block unauthorized access to trade secrets and confidential information, secure the information infrastructure from external attack, determine the effectiveness of IT control mechanisms, perform routine IT security audits, and prevent other IT activity that might compromise investor equity." With the proposed model that this study will present, this objective, one that has proved to be quite challenging for IT Departments to do, could be made an achievable one. Through Computer Information Systems, tools and methods of monitoring and measuring levels of compliance are now being reinforced. Should controls be not properly measured and compliance not enforced in companies and government agencies, the probability of fraud and unethical behavior is likely to be higher. As Ingram, et.al ([15] state "unethical behavior may occur in business because appropriate accounting controls are not in place or are not enforced". IT Controls can be defined as provisions or countermeasures taken by IT and the Corporation or Institution's Higher Management to minimize or mitigate risk and to ensure the clarity and effectiveness of the operation. When proper Security or Application Controls are missing, not ensured or simply inconsistent with each other, failure in the Security Effort arises when and internal or external audit is conducted on IT operations, leading to what Bassett [4] says that if necessary application controls are missing, it poses a serious security risk to the company 's customer service activities. Sometimes these missing controls are the result of faulty programming code during the software development phase [4]. Therefore IT Governance becomes a difficult task when proper IT and application controls are missing or inadequate.

The political pressures to implement efficient, quick and cost-effective solutions as well as the ability to adapt to current trends forces the companies and agencies to speed up operations, leaving controls design and assurance last, as shown in Figure 1.

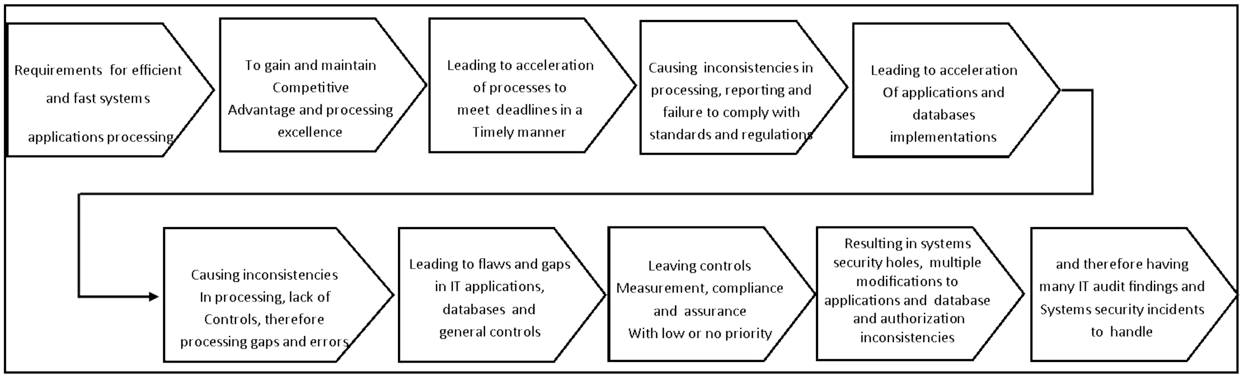
Requirements for efficient and fast systems applications processing
To gain and maintain Competitive Advantage and processing excellence
Leading to acceleration of processes to meet deadlines in a Timely manner
Causing inconsistencies in processing, reporting and failure to comply with standards and regulations
Leading to acceleration Of applications and databases implementations
Causing inconsistencies In processing, lack of Controls, therefore processing gaps and errors
Leading to flaws and gaps in IT applications, databases and general controls
Leaving controls Measurement, compliance and assurance With low or no priority
Resulting in systems security holes, multiple modifications to applications and database and authorization inconsistencies
and therefore having many IT audit findings and Systems security incidents to handle

Figure 1. The Path to IT Controls Vulnerabilities

This study on IT Governance will explore the possible causes for poor IT control validations, parameter settings and maintenance during each phase of an application development and implementation project, as well as the state of general IT controls within Puerto Rico' government agencies. The specific levels of validation and testing will be explored. Validation programs and selection criteria is an essential but complex part of any application development. This could be the reason why these activities most of the times have medium or low priority and when Projects fall behind Schedule or running out of budget, validation testing is even overlooked. This is also why this study intends to dig deep into the data validation standards and evaluate its effectiveness in light of the current trends presented in chapters 1 and 2 (Enterprise Resource Planning (ERP) and Service Oriented Architecture (SOA)). Two sample application model structures will be used during the study.

Peltier [20] states that an application control should consider design and implement application controls such as data entry checking, fields requiring validation, alarm indicators, password expiration capabilities, checksums and others, to ensure the integrity, confidentiality and availability of application information. He also states that Acceptance Testing must comprise develop testing procedures to be followed during applications development and during modifications to the existing application that include user participation and acceptance. During this study a bottom-up approach of Application controls analysis, design, coding or establishment and later maintenance will be made, starting with the systems analysis phase of the System Development Life Cycle (SDLC) and its role during the project management planning stage activities. The SDLC model will be evaluated and compared with the Project Management Model with a focus on controls and parameters setup and evaluation. Systems Security parameters will be evaluated as well. The new trend for application development called Service Oriented Architecture (SOA) will be studied, as it is part of the bottom-up approach of the present study. This emphasizes on Data Modeling and Parameters settings while modeling the data and work flows.

The sequence of activities constitutes a data flow or information flow. A top-down flow originates from events that occur at the top management level in an organization. Systems record these events, summarize them, and report them to employees at lower levels. A bottom-up approach happens when events occur at lower levels. These are recorded, summarize and then reported to top level. It depends on the organization culture structure or ways of doing business that provides which information flow will be followed.

In our bottom-up approach to compliance reporting we will evaluate:

- What basic standard controls should be established?
- How it escalates?
- How it is logged?
- How to ensure that it is clearly documented?
- How it is reported?
- How security measures are integrated?
-

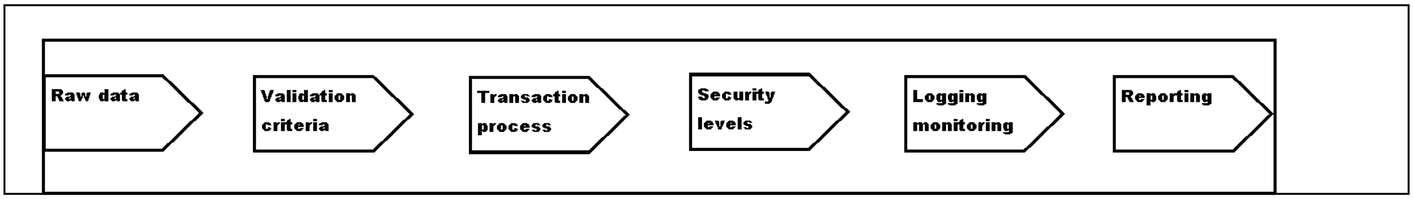

Figure 2. Basic Data Flow

A recent survey among CIOs and IT experts, where they were asked to rank the top eleven IT controls, showed that application controls and quality assurance weren't selected among them. Only data input controls was ranked the 11th. Among the conclusions of their study was noted that small businesses are not likely to be familiar with file access privilege controls. Since applications of information technology are not transparent, management is sometimes unaware of what is actually running in the system and its applications (MIS and Systems Security included). It is a harsh reality that will be evaluated as well.

Therefore a basic flow was depicted and the following were studied:

- Evaluate the present condition in application design steps/methodology. We'll specifically look at all activities that happen in the process and how they are reported. To accomplish this, tools like Data Models, Data Flow Diagrams (DFD), Entity Relationship Diagrams (ERD) and Flowcharts will be used.
- Evaluate precision in parameter and validation rules definitions, design, implementation and testing, and establish how they will be addressed in the study.
- Propose what will be the new model and its use for local small business, public corporations and government agencies in Puerto Rico, which lacks a formal, control IT infrastructure regulations and formal policies, as well as compliance reporting standards.
- Present a framework for IT Governance adjusting it to the current needs and operational environment of Puerto Rico's government agencies.

An analysis of the current Puerto Rico Law Project and Office of the Comptroller standards for information systems audit was conducted along with standards from the Office of Ethics Management, Financial Institutions Commissioner's Office, and Insurance Commissioner's Office. A tendency analysis & frequency distribution was performed. Data models and control statements were studied, mainly from public documents, studies and previous researches. We also evaluated their level of understanding of what must be required and included in every IT application in production and to be developed. Then the methodology and tools required and currently used to achieve the proposed objective of IT Applications Controls Correctness and validity was studied, as well as the Systems Security Professional awareness and procedures that needs to be in place to help achieve this objective. The awareness level of the application design and to what extent IT Directors (MIS) and Systems Security Managers are aware of what is really running in their systems was measured by administering a questionnaire. The instrument did not gather any personal, or agency information to ensure objectivity in the responses given to it. An internal control questionnaire asked a series of questions about the controls in each audit area as a means of indicating to the security officer, compliance officer or auditor aspects of internal control that may be inadequate. The procedures to test the effectiveness of controls in support of a reduced assessed control risk are called tests of controls.

The questionnaire was administered to a sample of one hundred (100) Information Technology Professionals. The sample was selected by convenience, as designated by the sample agency's executive director or MIS prerogatives. Expert professionals (both former and current CIOs) and Security Professionals from the government agencies and the collaboration of the Information Systems Audit and Control Association Puerto Rico Chapter were also included. The independent variables are controls, technology (SOA, ERP), project management models and the role of the security officer. The dependent variable has been defined as IT Governance. To measure these variables, a tendency measure analysis, specifically percentages and proportions analysis was performed.

By looking at the procedure and then evaluating its cause and effect, it was ensured that the standards for design, validation, execution and generation developed will be one of high quality. Also by studying the data flow through various channels from a security standards perspective the following questions are addressed: how it is stored, reported and kept secure. The various systems will achieve a level of reliability and trust where all higher and middle management could feel confident in certifying and audit procedures will be a smooth process instead of a nightmare as sometimes is for some companies or government agencies. The focus of making CIOs and CSOs be aware of the importance of IT Controls as the main vehicle for compliance, sound management, secure infrastructure and trustable results were primary for the present study.

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 changed. The main objective behind this piece of legislation was to turn the CIO from the technology guy/gal 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.

Today's complex IT projects must be directed by highly trained, technical and managerial people. 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 many procurements 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.

The Commonwealth of Puerto Rico's Constitution of 1952 established the current government structure. The executive power names the judiciary power, composed of the Puerto Rico Supreme Court, District and Municipality Courts and the third power if the legislative chamber composed of the Senate and the House of Representatives. The government is composed of 160 agencies and public corporations employing approximately 350,000 employees. Every agency's executive director or president names their staff for up to 25 employees.

The design of output and input structure for a system or application is critical to the successful implementation of an Enterprise Application System because it is the output which provides the information to the end-users of the enterprise, agency or institution and is the basis for the justification of the overall operating environment. Based on the outcome, output analysis and initial design, the input data model can be then depicted accordingly. This ensures that all necessary raw data needed to produce the desired output is included. The analyst/developer must spend considerable time and effort in determining what information must be generated from the process and the input data needed and the possible sources of input as well as the output methods. The analyst/developer must also determine data that will be stored on auxiliary storage for use by the system. For this the initial data modeling tools that would aid in effective data selection, validation and inclusion within the database tables would be Data Flow Diagrams (DFD's) and Entity Relationship Diagrams (ERD) following careful definition of Business Rules. From this a Data Dictionary is then modeled.

Some MIS argued that the DFD's are no longer necessary since no JCL's or operator's run books are longer needed. Thus some MIS associated to mainframe-type operations where process-flow diagram, system flowcharts were a necessity and required in operator's run book. The Puerto Rico Office of the Comptroller (www.ocpr.gov) 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 in 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

The results have been tabulated in Table 1.

Table 1

Findings	2001-2002	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007	Totals
A	11	12	2	12	9	11	57
B	3	14	2	2	4	7	32
C	2	11	4	13	8	12	50
D	4	9	2	7	8	5	35
E	11	13	8	10	6	5	53
F	14	13	7	9	22	30	95
G	13	15	14	3	12	5	62
H	3	4	8	1	11	7	34
I	0	2	2	1	1	1	7

Based on the above findings, we make the following recommendations. The Governor's Information Systems Audit Committee should be expanded and meet at least monthly. The State 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 is there; it only 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 Puerto Rico 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.