IT Governance and Internal Controls to Comply with Laws and Regulations

Milton Rojas Acevedo
Computer Science
Juan Ramírez, Ph.D.
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— Laws and Regulations affect how Organizations conduct their day to day operations. Before implementing any type of procedures, organizations must be aware of these regulations. In those cases were procedures are automatized and/or computerized, how does management assure that Laws and Regulations have been taken into consideration when a new system has been developed or acquired. In order to optimize computerized and/or automatized business process, management has to understand and implement adequate levels of IT Governance. With an appropriate IT Governance framework, IT Internal Control may be put in place to protect the integrity, confidentiality and availability of information systems, and thus, comply with established Laws and Regulations.*

Key Terms *— Confidentiality, Integrity, IT Governance, and IT Internal Controls.*

INTRODUCTION

IT related functions have become an integral part of business processes in how organizations reach their goals and objectives. Nowadays, an organization cannot operate without applications, network/infrastructure, and/or databases.

What is the best way to optimize and guarantee that IT functions will be aligned with business goals and objectives – IT Governance. With an adequate management of IT objectives and resources, any organization can assure that their IT objectives are aligned with their organizational goals. With the implementation of suitable IT internal controls, organizations will increase the probability of achieving business objectives.

In this article, an explanation of what is IT Governance, as well as IT controls will be presented, considering the importance of Laws and Regulations to demonstrate how IT Governance and effective IT controls are implemented, not only to comply with regulation, but to optimize business and operating functions.

IT GOVERNANCE

The IT Governance Institute defines IT Governance as the responsibility of the board of directors and executive management. [1] It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives. [2]

IT Governance focuses on the following aspects of management, as established by COBIT 4.1: Strategic Alignment, Value Delivery, Resource Management, Risk Management, and Performance Measurement. Refer to Figure 1 for an illustration of the IT Governance focus areas, as explained by COBIT 4.1:

Figure 1
IT Governance

A strong and effective IT Governance framework allows for Organizations to be aligned with Laws and Regulations such as SOX and HIPAA.

Some of these benefits include [1]:

- Gain competitive advantage through more efficient and effective operations.
- Enhance risk management competencies and prioritization of initiatives.
- Enhance the understanding of IT among executives.
- Optimize operations with an integrated approach focused on security (confidentiality, integrity and availability).
- Enable better business decisions by providing higher-quality.
- Align project initiatives with business requirements.
- Prevent loss of intellectual assets and the possibility of system breach.
- Contribute to the compliance of other regulatory requirements, such as privacy.

An effective IT Governance methodology focuses on realizing benefits by increasing automation and optimizing an enterprise creating it more effective, by decreasing cost and enhancing operational procedures. [2]

Figure 2 demonstrates how an effective IT Governance Framework facilitates an organization and helps meet their strategic goals and objectives: [2]

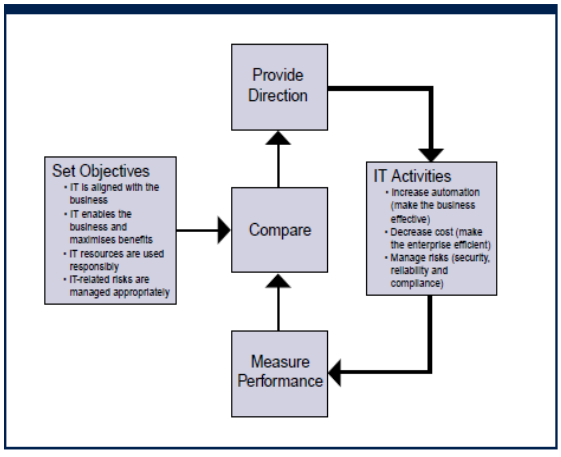

Figure 2
IT Governance Framework

The IT governance structure should be designed so that IT adds value to the business and IT risks are mitigated. This also includes an IT organization structure that supports adequate segregation of duties and promotes the achievement of the organization's objectives. [1]

In order for organizations optimize their IT internal controls through an efficient IT Governance framework, the following three elements must be in place:

- Executive Management: establishes and incorporates strategy into business activities develop business strategies, policies and decisions are made on how to deploy and manage organizational resources. [1]
- Business Process: creating and delivering value to stakeholders through the effective business operations. [1]
- IT Services – when business process is automatized, IT services forms the foundation for optimizing operations, through services such as network management, database management, operating system management, storage management, facilities management, and security administration. [1]

Considering the growing importance in IT Governance to assist business units in achieving their strategic goals and comply with Laws and Regulations, the implementation of effective and efficient IT Controls is essential.

IT CONTROLS

IT Controls, and controls in general are procedures and/ or activities to ensure that specific business functions are met. IT Controls are generally associated with Information Security, to optimize and protect the integrity, availability and confidentiality of sensitive information assets. Effective controls reduce risk, increase the likelihood of value delivery and improve efficiency because there will be fewer errors and a more consistent management approach. [13]

The most important IT controls can be implemented in the following areas of IT: computer

operations, access to programs and data, program development, and program changes. [1]

Although these are some broad areas of IT, Institutions that focus their IT controls on these areas may have a Top-Down approach to ensure that every critical function has an appropriate IT Control associated. IT Controls must be robust enough to address and/or mitigate any risk associated with procedures that manage sensitive date such as financial data, non-public personal information, or any other information asset deemed critical to business functions.

Computer Operation

Controls over the day-to-day operations of information services may include service-level management, management of third-party services, system availability, incident management, customer relationship management, and systems management. [1]

Controls should be put in place to guarantee that computer operations are optimized and adequately allow for proper business operation. Institutions should include performance metrics that define minimum service level requirements and remedies for failure to meet those agreed upon standards. For example, common service level metrics include percent system uptime, deadlines for completing batch processing, or number of processing errors. [3]

Institutions or Organizations that depend on IT services, especially processing financial data, should establish accurate and formal Service Level Agreements (SLAs). SLAs are formal documents that outline the institution's predetermined requirements for the service and establish incentives to meet, or penalties for failure to meet, the requirements. [3]

Although agreed upon SLA's vary between organizations, depending on their need and depending if the service being provided (internal or outsourced), the following issues, at a minimum, should be addressed [3]:

- Availability and timeliness of services;
- Confidentiality and integrity of data;
- Change control;
- Security standards compliance, including vulnerability and penetration management;
- Business continuity compliance; and
- Help desk support.

Management should be aware of the different types of risks associated with IT services. Such risks depend on how the service is being provided, the criticality of the data being processes, as well as the maturity level of the process being performed. It is for these reasons that Organizations should establish controls were monitoring performance (against SLAs) and incident management is appropriately implemented. Risk associated with third party providers are augmented by the nature of the relationship. Contracts should be in place to protect the integrity, availability, and confidentiality of data and information shared with a third party.

Management should consider implementing contract provisions that address the following controls: Service provider internal controls; Compliance with applicable regulatory requirements; Record maintenance requirements for the service provider; Access to the records by the institution; Notification requirements and approval rights for any material changes to services systems, controls, key project personnel, and service locations; Setting and monitoring parameters for financial functions including payments Processing or extensions of credit on behalf of the institution; and Insurance coverage maintained by the service provider. [3]

Besides the above mentioned clauses in contracts, one of the most important aspects of Computer Operations is its system's availability. Unavailable critical systems may result in losses and penalties to any Institution. Considering the importance of availability, system uptime is a crucial and essential aspect when establishing and implementing Internal Controls. [4] The best way to assure system availability is through Contingency planning through and an adequate Business Continuity Plan [5].

Contingency Planning is the process of creating a plan that will be activated when normal operation is obstructed. Contingency planning may be defined as: documentation prepared by the organization to

anticipate, react to, and recover from events that threaten the security of information and information assets in the organization, and, subsequently, to restore the organization to normal modes of business operations. [4]

Adequate internal controls should be implemented to address every one of these issues to sustain normal operations.

Access to Program and Data

Controls associated with access to programs and data address system access issues (least privilege, Segregation of duties), effective passwords implementation, Firewalls, and data encryption. By preventing unauthorized use of, and changes to, any system, the integrity of every data is maintained.

Ever since the beginning of information security, access control has been in the forefront of security controls. The concept is simple, restrict access to unauthorized users. The least access acceptable in order to conduct the task is considered best practice. [6]

Access Control is one of the most important aspects of computer security. A simple process of Access control begins with a subject trying to obtain access to a specific resource (object). [7] The subject is first authenticated (Verifying if the user is valid), after being authenticated the user will now be authorized (given permission to a certain resource). The access control function consults with the authorization database to determine whether to grant access.

The Access Control Policies can be divided in the following categories: [7]

- *Discretionary Access Control (DAC)*: Controls access based on the identity of the requestor and on access rules stating what requestors are allowed to do. It is discretionary because an entity might have access rights that permit that entity, but cannot enable another entity to access that resource.
- *Mandatory Access Control (MAC)*: Control access based on comparing security labels with security clearance. It is termed mandatory because an enable user does not have the right to enable another user.
- *Role-based control (RBAC)*: Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

In order to optimize internal controls, access to sensitive information is crucial. These access control techniques should provide Institutions the means to protect information assets and abide by the Laws and Regulations that affect them. It is for this reason is why internal controls follow the best practices of least privileges and Segregation of duties.

The concept of least privileges implies that a subject should only have sufficient access (or privileges) to perform those tasks assigned. [8]

The concept of Segregation of Duties refers to establishing controls to prevent any single employee (or user) to perform a complete task individually.

Successful access control systems must implement controls with robust and adequate authentication and authorization (verification) mechanisms. User Authentication as the process of verifying an identity claimed by or for a system entity. [7] This process consists of two steps; Identification and Verification. The Identification step is defined as presenting an identifier to the security system and Verification step is defined as presenting or generating authentication information that corroborates the binding between the entity and the identifier. A simple example of user authentication is providing user name and password. A user name provides identification, and the password verifies the correct user, thus completing both steps of user authentication.

Considering the rise in sophistication of malicious intruders, for authentication purposes, it is considered best practice to implement at least two forms of authentication to authenticate the subject's identity.

There are four means of Authentication which are the following: Something the individual knows: Password or a PIN number; something the individual possesses: Smart cards or electronic keys. These kinds of authenticator are referred to as Tokens; something

the individual is (Static Biometric): Finger print or retina; something the individual does (Dynamic Biometric): Recognizing voice pattern, handwriting. [7]

Although it may seem trivial, one of the most essential controls is the implementation of effective passwords. Password serves to authenticate a user logging into a system. User accounts provide security by determining whether the user is authorized to gain access, the privileges accordingly, for discretionary access control.

One of the most fundamental problems with passwords is that users create them too simplistic and easy to "crack". The simplicity of the passwords is what allows hackers to predict them. If password are created randomly, it would be improbable (considering other password parameters as length and complexity) for the hackers to guess. This cannot be done given that it would be practically impossible for the users to always remember randomly selected characters as a password. The goal when implementing adequate password controls is to eliminate guessable passwords while allowing the user to select a password that is memorable. Some basic techniques to use are: [7]

- Employee Awareness (User Education)
- Computer-generated passwords
- Reactive password checking
- When the system periodically runs its own password cracker to find guessable passwords.
- Proactive password checking
- User selects the password but the system checks to see if the password is allowed rating the level of simplicity.

Although sometimes misconceived as the ultimate layer of security, firewalls, although essential, are not all inclusive. The truth of the matter is, for firewalls to be effective; they need to be combined with other security methods and techniques. With that said, firewalls still compose an essential aspect of information security and IT Controls.

Firewalls have different types of categorization, but firewalls categorized by processing mode are; packet filtering, application gateways, critical gateways, MAC layer firewalls, and hybrids. [6]

Besides firewalls, another essential and very effective IT Control practices are the implementation of Encryption, albeit in transit and/or stored. Encryption is one of the most important aspects of Information Security, and should be implemented by every Institution as part of their internal controls.

Encryption may be defined as: converting original message into a form unreadable by unauthorized individuals. [6] In essence, the purpose of encryption is to disguise data or information (usually sensitive); using a combination of keys and algorithms, to make it unreadable to unauthorized users.

Encryption has two major categories; symmetric and asymmetric encryption. In the case of symmetric encryption, one key is used to communicate with both parties, the same key is used to encipher as to decipher. [6]

It is important to emphasize that the most important aspect of encryption is the key. The size of the key determines the complexity and the robustness of the encrypted message. Many times, the algorithms used to create encrypted messages, are made public, but the key is not. It is very important that the key is kept secure, in order to retain effective encryption.

Combining both types of encryption methods may improve certain typed on internal controls. Nonetheless, encryption should be established to sensitive data, (based on criticality).

Program Development and Program Change

Organization should also be aware, and implement controls associated with systems Development and Acquisition, as well as maintenance of existing applications. Development and acquisition is an organization's ability to identify, acquire, install, and maintain appropriate information technology systems. [9]

Lack of internal controls associates with systems development and acquisition may result in losses due to inadequate processes, personnel or systems, which include errors, fraud or inability to deliver products and/or services.

The most efficient manner to appropriately handle system development and acquisitions is to establish project management controls. One of the most important project management techniques is the System Development Life Cycle (SDLC). Organizations may employ an SDLC model or alternative methodology when managing any project, including software development, or hardware, software, or service acquisition projects. [9]

The System Development Life Cycle intends to break a big project, into smaller and manageable phases. The phases vary between objectives and complexity, but generally are divided as follows; Initiation phase, Development/Acquisition phase, Implementation / Assessment phase, Operation / Maintenance phase, and Disposal phase.

Refer to Figure 3 taken from the NIST Security Considerations in the Systems Development Life Cycle publication which demonstrates a conceptual view of the System Development Life Cycle (SDLC). [10]

Figure 3
SDLC Conceptual View

- *Initiation Stage*: The initiation phase begins when an opportunity to add, improve, or correct a system is identified and formally requested through the presentation of a business case. [9] The purpose of the business case is to demonstrate to senior management how the new system would benefit the organization. Benefits may be obtained in different ways, such as, monetary, operational, or reputational. Once a business case is acknowledged and approved, a thorough feasibility study must be performed to analyze the potential benefits against the presumed cost. Primary issues organizations should consider when compiling feasibility study support documentation include: Business Considerations; Functional Requirements; Project Factors; and Cost/Benefit Analysis.
- *Development/Acquisition phase*: Once the initiation phase is complete, and the business case has been approved by senior management. The next step in the SDLC is the Development or Acquisition stage (depending if it is going to be developed in house, or acquired externally.
- *Implementation/Assessment phase*: Once the expected system has been developed or acquired, the implementation phase may begin. The implementation phase involves installing approved applications into production environments. [9] During the implementation and assessment phase many of the system requirements will be tested and evaluated in the operational environment. [10]
- *Operation/Maintenance*: The maintenance phase occurs after the newly developed system has been developed/acquired and implemented. The maintenance phase involves making changes to hardware, software, and documentation to support its operational effectiveness.
- *Disposal phase*: The final phase of the SDLC is the Disposal phase. The disposal phase involves the orderly removal of surplus or obsolete hardware, software, or data. Primary tasks include the transfer, archiving, or destruction of data records. [9]

Now that IT techniques and methodologies have been discussed in IT Control environments, an explanation of how these controls must be managed in order to comply with Laws and regulations such as SOX, HIPAA and PCI.

SARBANES-OXLEY ACT OF 2002

As a result of many internal frauds and accounting scandals such as Enron, WorldCom and Tyco International, the Sarbanes-Oxley Act, most

commonly known as SOX came about. This act intends to regulate how financial practices are performed on US public companies.

The act, in itself, has eleven "titles" which enforce corporate board responsibility as well as penalties for those non-compliant; however, two sections within those titles pertain to IT internal Controls and internal controls in general.

These sections are: Sec. 302- *Corporate Responsibilities for Financial Reporting, Sec. 404- Management Assessment of Internal Controls*.

In summary, Sec. 302 implies that quarterly and annually, financial officers (or the corresponding individual) must sign off (acknowledge) that they are aware of the financial statements being emitted, and the conditions presented are the actual status of the Institutions. The corresponding officer also acknowledges awareness of internal controls, and that any lack of compliance has been reported. [1]

Sec. 404 implies that internal controls are in place, tested and addressed if necessary. In the Institutions' annual report, officers should include information regarding to the adequacy and scope of its implemented internal controls. [1]

Although SOX has been implemented to rule over financial conditions, in today's organization many, if not all, financial data is processed through computerized or automatized information systems. It is for this reason that IT Governance and IT controls has taken immense consideration and is evaluated with such attention to comply with Laws and regulations, such as SOX.

The Sarbanes-Oxley Act makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. [1] For most organizations, the role of IT is crucial to achieving this objective. IT is the foundation of an effective system of internal control over financial reporting. [1]

Many organizations need IT members when evaluating SOX controls considering that IT is such a large part of how financial data is processed and generated. Some of the important areas of responsibility for IT include: [1]

- Understanding the organization's internal control program and its financial reporting process.
- Mapping the IT environment (IT services and processes) that supports internal control and the financial reporting process to the financial statements.
- Identifying risks related to these IT systems
- Designing and implementing controls designed to mitigate the identified risks and monitoring them for continued effectiveness.
- Documenting and testing IT and systems-based controls.
- Ensuring that IT controls are updated and changed as necessary to correspond with changes in internal control or financial reporting processes
- Monitoring IT controls for effective operation over time.
- Participating in the Sarbanes-Oxley project management office.

It is for these reasons that IT controls must be generated, implemented, and periodically tested by organizations.

In order to be fully compliant with SOX requirements, the following guidelines are suggested: [1]

- Plan and Scope IT Controls:
  - Inventory relevant applications and related subsystems (matrixes, inventories).
  - Review Financial Process Documentation and Identify Application Controls.
  - Determine responsibility for application controls (data owner, application administrator).
  - Determine dependencies on third parties (assure that SSAE 16 evaluate SOX controls).
- Assess IT Risks:
  - Assess Inherent Risk of Applications (Risk Assessment).
  - Refine Scope and update plan.
- Document Controls:
  - Identify IT Entry-Level Controls
  - Identify Application Controls (balancing control, check digits, reasonable tests, logic tests, calculations).

- Identify General Control (access controls, configuration changes) – Refer to Appendix I for a list of General Controls.
- Control Documentation.

- Evaluate Control Design and Operating Effectiveness.
  - Evaluate Control Design.
  - Evaluate Operational Effectiveness.
  - Consider the Nature of Evidence Required.
  - Consider the riming of Control Testing.
- Prioritize and Remediate Deficiencies.
  - Identify and Assess IT General Control Deficiencies.
- Build Sustainability.
  - Automate Controls.
  - Perform Application Benchmarking.

The following illustration provides a roadmap for the SOX compliance requirements just mentioned. Refer to Figure 4 for the SOX Roadmap: [1]

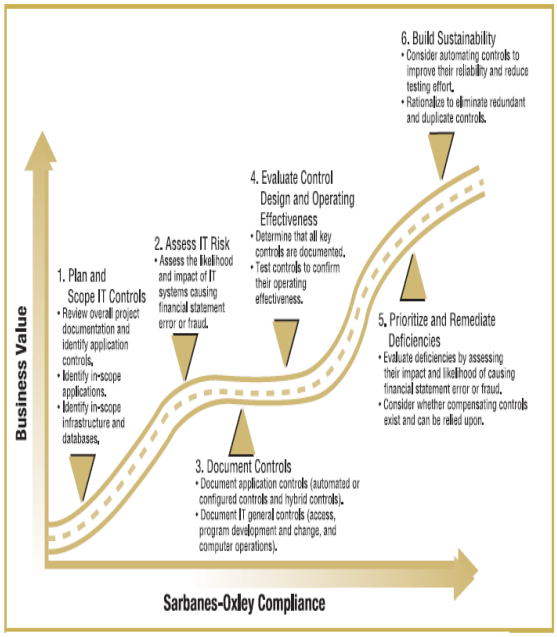

Figure 4

OX IT Compliance Roadmap

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The U.S. Department of Health and Human Services explains the HIPAA as follows: The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety. [15]

The very nature of medical technology represents significant threats to IT Governance and IT Controls on a medical facilitate. Considering the heterogeneous environments of systems; ranging from different manufacturers to different types of equipment present added risk to IT security.

Implementing adequate IT Controls may be challenging when organization must also abide by the HIPA Act.

ISACA (known as Information Systems Audit and Control Association) has submitted an article on their 2008 volume 6 journal on several practices and/or guidelines for implementing IT Controls to abide by the HIPA Act. The Guidelines stated were as follows: [16]

- Establish a VPN Connection
- Implement Segregation of Duties
- Establish adequate Access Controls
- Tracking and reporting user activity
- Testing and reporting controls

For each of these controls, if an IT Governance framework is established correctly, compliance with the HIPA Act will be attained. As with SOX requirements, secure access is essential to protect the confidentiality of the date, and thus the clients' medical-personal information.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

The PCI DSS was introduced in 2001 by Visa USA. The main objective of the standard was to reduce large-scale credit card compromises in e-commerce web sites, acquiring organizations and merchants. [11]

The PCI Security Standards Council defines the PCI requirements as security standards are technical

and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council, American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. [12]

Refer to the following illustration (Figure 5) which demonstrates the PCI Security Sections and Standards: [11]

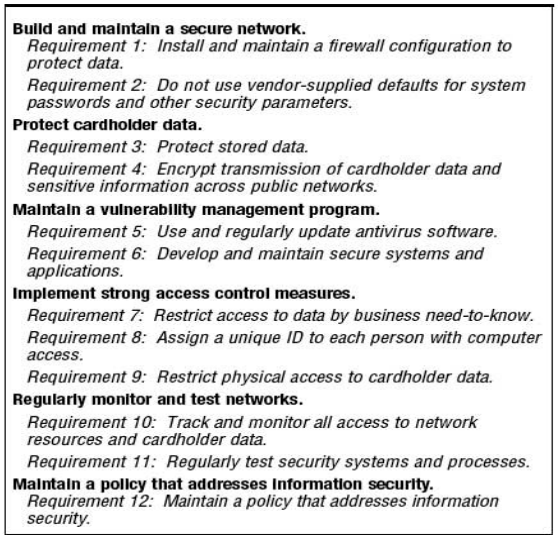

Figure 5
PCI Security Sections and Standards

In order to comply with PCI standards, many organizations utilize several frameworks to facilitate the implementation of internal controls. One of the most popular frameworks which maps control requirements to business need is the Control Objectives for Information and Related Technology (COBIT), by ISACA.

COBIT provides good practices across a domain and process framework and presents activities in a manageable and logical structure. [13]

With COBIT (4.1) a mapping can be reached to assure that every PCI Security Section and Standard has an established Control Objective.

- *Requirement 1*: Install and maintain a firewall configuration to protect data, the following COBIT Control Objective can be implemented to comply with this requirement: Security Testing, surveillance and Monitoring; Protection of Security Technology; Network Security; and IT Infrastructure monitoring. [14]
- *Requirement 2*: Do not use vendor-supplied defaults for system passwords or other security parameters: Security Testing, Surveillance and Monitoring and; Protection of Security Technology. [14]
- *Requirement 3*: Protect stored cardholder data: Data classification schemes, Offsite backup storage Cryptographic key management, and Security requirements for data management. [14]
- *Requirement 4*: Encrypt transmission of cardholder's data across open public networks Cryptographic key management, Network security, Management of IT security, and Protection of security technology. [14]
- *Requirement 5*: Use and regularly update antivirus software on all systems commonly affected by malware: Malicious software prevention, detection, and correction. [14]
- *Requirement 6*: Develop and maintain secure systems and applications: Develop and acquisition standards, Risk Assessment, Feasibility maintenance, Change standards and procedures, Impact Assessment, periodization and authorization. [14]
- *Requirement 7*: Restrict access by business to cardholder's data to need to know basis: Identity management, User account management. [14]
- *Requirement 8*: Assign a unique ID to each person with computer access: Identity Management, User account management, Job change and termination, Protection of security technology. [14]
- *Requirement 9*: Restrict physical access to cardholders' data: Responsibility for risk, security and compliance, User account management, Physical access, Physical security measures, and Storage and retention arrangement. [14]

- *Requirement 10*: Track and monitor all access to network resources and cardholder data: Security testing, surveillance and monitoring, IT Infrastructure monitoring. [14]
- *Requirement 11*: Regularly track security systems and processes: Event Identification, Security Incident definition, Definition and collection of monitoring data, Monitoring of internal control framework, Control exceptions, and Remedial actions. [14]
- *Requirement 12*: Maintain an Information Security Policy: Policy, plans and procedures, IT Steering Committee, Organizational placement of the IT Functions, Responsibility for risk, security and compliance, IT Policies management, Management of IT security, and IT Security Plan. [14]

Complying with guidelines and regulations such as PCI can be cumbersome and challenging to many organizations. As long as efficient IT Governance and standards and/or framework, such as COBIT, are implemented, adequate controls may be implemented to comply with such regulations.

CONCLUSION

Considering the implied importance that is now part of IT related functions, it is imperative that Organizations invest, train and address IT Governance adequately. The Benefits are tangible and worth the investment.

IT Governance has become an integral part of Organization, and they should implement IT Governance strategies to optimize their business functions as well as to comply with regulations. By using the techniques in successful IT Governance Frameworks, Organizations will be able to align IT initiatives to strategic goals such as improving operations, lower maintenance, or reduce obsolesce. Successful frameworks such as ISACA's COBIT allow for Organizations to align objectives, measure performance, and allocate resources in a more efficient manner.

With successful IT Governance, and adequate IT Internal Controls, Organization will improve the way they comply with Laws and Regulation such as SOC and HIPAA. Although Laws and Regulations affect how IT Controls are implemented, they cannot, and must not, be the only reason to invest in successful IT Governance practices and IT Internal Controls.

REFERENCES

[1] The IT Governance Institute. (2006). IT *Control Objectives for Sarbanes Oxley- The Role of IT in the Design and Implementation of Internal Controls over Financial Reporting.* United States of America.

[2] The IT Governance Institute. (2003). *Board Briefing on IT Governance*. United States of America.

[3] Federal Financial Institution Examination Council. (2004). *FFIEC IT Examination Handbook; Outsourcing Technology Services*. Retrieved from http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

[4] Michael E. Whitman and Herbert J. Mattord. (2007). *Principles of Incident Response and Disaster Recovery*. Thompson Course Technology

[5] Federal Financial Institution Examination Council. (2008). *FFIEC IT Examination Handbook; Business Continuity Planning.* Retrieved from http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

[6] Michael E. Whitman and Herbert J. Mattord. (2005). *Principles of Information Security.* Thompson Course Technology

[7] William Stallings, & Lawrie Brown. (2008). *Computer Security: Principles and Practice*. Prentice Hall

[8] Federal Financial Institution Examination Council. (2006). FFIEC *IT Examination Handbook; Information Security*. Retrieved from http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

[9] Federal Financial Institution Examination Council. (2004) *FFIEC IT Examination Handbook; Development and Acquisition.* Retrieved from http://ithandbook.ffiec.gov/it-booklets/development-and-acquisition.aspx

[10] NIST Special Publication 800-64. (2008). *Security Considerations in the Systems Development Life Cycle*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf

[11] Woda, A. (2007*). Achieving Compliance with the PCI Data Security Standard*. Retrieved from: http://www.isaca.org/Journal/Past-Issues/2007/Volume-4/Pages/Achieving-Compliance-With-the-PCI-Data-Security-Standard1.aspx

[12] PCI Security Standards Council. (2010). *PCI DSS Quick Reference Guide*; Retrieved from

https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

[13] The IT Governance Institute. (2007). *COBIT 4.1 – Framework, Control Objectives, Management Guidelines, Maturity Models*. United States of America

[14] Bankar, P. (2011). *Mapping PCI DSS v2.0 With COBIT 4.1* Retrieved from; http://www.isaca.org/Journal/Past-Issues/2011/Volume-2/Pages/Mapping-PCI-DSS-v20-With-COBIT41.aspx

[15] U.S. Department of Health & Human Services. *Health Information Privacy. Retrieved* from; http://www.hhs.gov/ocr/privacy/

[16] Traverse, C (2008*). Implementing, Automating and Validating Controls for Privileged Users in Healthcare Organizations. Retrieved* from; http://www.isaca.org/Journal/Past-Issues/2008/Volume-6/Documents/jpdf0806-implement-automat.pdf