ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (125-150), Month: October - December 2014, Available at: www.researchpublish.com

An Information Technology Perspective on Sarbanes-Oxley: Past, Present, and Future

Charles D. Madewell

Abstract: **This article performs qualitative research of the most current thought and discussion concerning Sarbanes-Oxley. These thoughts and discussions are collected, analyzed, synergized, and presented as the output of this article. The article first gives a general introduction highlighting the new roles being placed upon Chief Information Officers and the value of companies maintaining a good perceived image. Then, the article discusses the laws leading to Sarbanes-Oxley. The key points of the act are discussed as well as the topic of governance and management design then follows. Next, the implications of policy are outlined and the connection between ethical behavior and Sarbanes-Oxley are deliberated. Then, an in-depth analysis of the Sarbanes-Oxley Act and the future of the act are detailed in relation to need, examples of misconduct, propensity for success, known weaknesses, potential replacements, overall assessment, and major changes needed. Finally, this article concludes that, although not perfect, Sarbanes-Oxley is viable and needed.**

I. INTRODUCTION

Moeller (2013) does a great job in starting off the discussion by presenting a concise description of the origins of the Sarbanes-Oxley (SOx) Act. In the years leading up to the early part of this century, there were regulation, policy, and laws that covered how a corporation or company should operate. For the most part, this had to do with the way that a company does its accounting and how it keeps it records. Thus, up to 2002, the focus was on the financial transactions that a company executed while operating. This covered the company operations in a broad sense and certainly did not focus on information technology (IT) investments. But, in 2002 the SOx Act was put into place in the United States (Moeller, 2013). The main reason the SOx Act was implemented was due to corporations such as Enron. Enron failed very suddenly and unexpectedly which gave investors almost no time to offload the stock before the company crashed. U.S. government investigators then researched the Enron failure (along with other company failures of the time) and found that many governance and financial practices were not functioning as they should have been (Moeller, 2013, p. 4). Therefore, the U.S. government put in place legislation and law to invoke rules that U.S. companies shall follow regardless of their location. This law had major impacts on IT investments within companies and therefore Chief Information Officers now had to pay attention to SOx.

Maizlish and Handler (2005) point to Section 404 which are the internal controls required by SOx. These internal controls include: statement of management responsibility, manager's assessment of effectiveness, statement identifying the framework used to evaluate, and, finally, the statement of registered public accountant that audited the company. Much of these requirements funnel directly to the need for the Chief Information Officer (CIO) to have in place a process for good IT portfolio management. Since the IT projects must now be aligned with business operations strategies and must produce value, the IT governance process has to make sure that only the most valuable IT projects get justified, approved, and implemented. Good IT governance must also cause the IT investments to become transparent so that they can be tracked and seen from beginning to end. This is the most major impact to IT and to the CIO.

Moeller (2013) points out that good IT governance as required by SOx addresses the total end-to-end business processes. It also requires that coordination be done with the activities of the enterprise as well as across the whole organization. Thus, SOx impacts the whole company and the whole enterprise from top to bottom. With new requirements come the need for new compliance checks and audits. These new compliance checks and audit mechanisms are the responsibility of the whole company but often fall upon the CIO to insure that the checks and audits are being done. It also means that the company and the CIO have to find frameworks and methodologies to insure compliance. Often, methods like COBIT, COSO, ITIL, and ISO are used (Moeller, 2013, p. 5).

A company must be perceived to have good ethical conduct to also be perceived as ethical. This means that the company must operate with integrity and trust as well as act on the behalf of the stockholders. To have good ethical conduct, a company must design in auditing mechanisms to insure compliance. These auditing mechanisms help bring about and maintain good ethical conduct over time. This is where ethics is tied to SOx – the compliance mechanisms. Reynolds (2012, p. 64) points out that there are two primary auditing bodies. These are the auditing committee and the internal auditing team. Reynolds (2012) further points out that the overall goal of the auditing committee as well as the members of the internal auditing team is to ensure that both IT organizations and IT users are in compliance to the policies and procedures of the company as well as laws and regulations. This includes SOx. Thus the overall value and correlation to SOx is to keep the company in compliance which helps the company to be perceived as ethical or having a good ethical design in place. This paper will discuss the history, value, and future of SOx.

II. LAWS LEADING TO SARBANES-OXLEY

From as early as 1913, there have been acts passed to attempt to drive businesses to do the right thing and to be financially responsible to the stockholders and investors (Rockness & Rockness, 2005). Moeller (2013) points out that in the years leading up to the early part of this century, regulations, policy, and laws existed but focused on how a company should operate. Up to the Sarbanes-Oxley (SOx) Act of 2002, the acts had more to do with the way each company was to do its accounting and how it should keep the records. The focus was really more on financial transactions than anything else. Prior to SOx, there were eight acts that were passed as legislation. (Rockness & Rockness, 2005, pp. 34-35) discuss them as being: Owen-Glass Act of 1913, Glass-Stegall Act of 1933, U.S. Securities and Exchange Act of 1933, U.S. Securities and Exchange Act of 1934, Investment Company Act of 1940, Foreign Corrupt Practices Act of 1977, FIDCA Improvement Act of 1991, and the Private Securities Litigation Reform Act of 1995. Not included in these acts were the recommendations of the Securities and Exchange Commission (SEC). Reynolds (2012) notes that as early as 1972, the SEC was recommending that publicly held corporations should establish the role of an auditing committee. Each of these acts mentioned above has specific goals and requirements and many of them overlap with SOx in some fashion. Two acts which have very similar requirements to SOx are the U.S. Securities and Exchange Act of 1934 and the FIDCA Improvement Act of 1991.

U.S. Securities and Exchange Act of 1934: This act was similar to SOx in that it tried to invoke ethical behavior in financial transactions. The act requirements included: self-policing, filing quarterly, and auditing by registered companies on an annual basis (Rockness & Rockness, 2005). Much like this act, SOx also required more internal controls to self-police as well as very strict requirements on what reports and certifications must be filed as well as the use of auditing and the auditing committee. The U.S. Securities and Exchange Act of 1934 seemed successful for the time and was a necessary incremental step to SOx. But, SOx seems to do a much better job of specifying the exact requirements, the credentials of the auditors, and the required certifications, forms, and prohibited actions. Although both seem successful, SOx seems to be a better and more thorough act than the U.S. Securities and Exchange Act of 1934.

FIDCA Improvement Act of 1991: This act was also very similar to SOx. Much like SOx, the FIDCA Improvement Act of 1991 was much more thorough than earlier acts prior to 1991. This act was written to stop fraud and conflicts of interest by the directors and managers of corporations that were failing. So, this is indeed very similar to SOx. The particular requirements of FIDCA Improvement Act of 1991 include: required reports by officers on the internal controls and compliance as well as the use of independent auditors to attest to manager's reports and internal controls (Rockness & Rockness, 2005). These are exactly the very same two broad requirements within SOx. The SOx act requires that internal controls be used and that verification of compliance be made. SOx also requires that the compliance be attested to using independent certifications as well as the managers and employees attesting that the data they are giving is accurate and true. The SOx act also specifies the use of internal auditing committees as well as the executive auditing committee. So, both the FIDCA Improvement Act of 1991 and SOx have these requirements. Since SOx is more recent and more attuned to the current environment of corporate failures on a large scale, SOx seemingly does a better job and is more successful. The proof of this is that the FIDCA Improvement Act of 1991 already existed and SOx was still required to be passed because old acts were not getting the job done in the area of driving ethical behaviors and enforcing punishment on corporate executives who knowingly commit misconduct.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (125-150), Month: October - December 2014, Available at: www.researchpublish.com

III. KEY POINTS OF SARBANES-OXLEY

There are many good references that outline the key components of the Sarbanes-Oxley (SOx) Act of 2002. Of those, Rockness and Rockness (2005, pp. 43-44) do an outstanding job of listing the key components SOx by title and section. Moeller (2013, p. 11) and Romano (2005, pp. 1520-1540) also add to the list. All of these can also be found in United States Public Law 107-204 dated July 30, 2002 (United States, 2002). The key components are:

- **Title I, Public Company Accounting Oversight Board (PCAOB)**
  - Section 101, Establishment of the PCAOB
  - Section 104, Accounting Firm Inspections
  - Section 105, Investigations and Disciplinary Proceedings
  - Section 108, Auditing Standards
- **Title II, Auditor Independence**
  - Section 201, Prohibited Services/Out of Scope Practices
  - Section 203, Audit Partner Rotation
  - Section 206, Conflicts of Interest
- **Title III, Corporate Responsibility**
  - Section 301, Audit Committee Independence
  - Section 302, Corporate Responsibility for Financial Reports
  - Section 303, Improper Influence on Conduct of Audits
  - Section 304, Forfeiture of Certain Bonuses and Profits
  - Section 305, Officer and Director Bars and Penalties
  - Section 306, Insider Trades During Pension Fund Blackout Dates
- **Title IV, Enhanced Financial Disclosures**
  - Section 402, Enhanced Conflict of Interest Provision
  - Section 404, Internal Control Reporting
  - Section 406, Code of Ethics for Senior Financial Officers
  - Section 407, Financial Expert
  - Section 408, Enhanced Review of Financial Disclosures
  - Section 409, Real-Time Disclosure
- **Title V, Analyst Conflict of Interest**
  - Section 501, Treatment of Security Analyst by Registered Securities Associations and National Security Exchanges
- **Title VIII, Corporate and Criminal Fraud Accountability**
  - Section 802, Criminal Penalties for Altering Documents
  - Section 806, Protection for Employees of Publically Traded Companies who Provide Evidence of Fraud
  - Section 807, Criminal Penalties for Defrauding Shareholders of Publically Traded Companies
- **Title IX, White Collar Crime Penalty**
  - Section 903, Criminal Penalties for Mail and Wire Fraud
  - Section 906, Corporate Responsibility for Financial Reports

- **Title XI, Corporate Fraud and Accountability**
  - Section 1102, Tampering with Record or Otherwise Impeding an Official Proceeding
  - Section 1105, Officer or Director Prohibitions
  - Section 1105, Authority of the Commission to Prohibit Persons from Serving as Officers or Directors
  - Section 1106, Increase Criminal Penalties Under Securities Exchange Act of 1934
  - Section 1107, Retaliation Against Informants

Moeller (2013) outlines the main components related to IT and the CIO as including: Title I, Title II, Title III, and Title IV Section 404. Addison-Hewitt Associates (2006) give their opinion that the main components related to IT and the CIO include: Title III Section 302, Title IV Sections 401, 404, and 409 and Title VIII Section 802. Thus, there are multiple requirements within these key components that directly relate to IT and the CIO. For example, Addison-Hewitt Associates (2006) note that Title III Section 302 requires: the signing officers have reviewed the report, the report is not to contain any untrue statements, the financial statements and information present a fair picture of the condition, the signing officers are responsible for the internal controls, all deficiencies are to be listed, and note any significant change that could have a negative impact of internal controls.

Moeller (2013) does a great job of discussing the requirements for multiple key components of SOx. Title I Section 101 requires that the PCAOB administration and public accounting firm be registered, the auditing have independence standards applied, the audits be retained, and scope out the testing of internal controls. For Title IV Section 404, there must be compliance reviews that take into account: revenue cycles, direct expenditure cycles, indirect expenditure cycles, payroll cycles, inventory cycles, fixed asset cycles, and general controls for IT cycles. There is also a requirement to use the AS5 rules in the internal audit. These include: focusing on internal control audits that are most important, eliminating audits that are unnecessary, and insuring that the audit is fully scalable to fit the size and complexity of the company.

Moeller (2013) discusses the requirements for Title II as including: auditor independence and limitations on external auditor services. SOx prohibits the public accounting firm from providing these services: financial information systems design, book keeping statement services, management functions, human functions, and external audit firms offering actuarial services. Furthermore, the audit committee must preapprove services and must insure that the external auditing company is rotated at least every five years. This helps prevent conflicts of interest. Moeller (2013) describes the requirements for Title III as including a financial expert who can understand general accepted accounting principles, apply these principles, have experience in preparing and auditing financial statements, have experience with internal controls, and understand the audit committee functions.

Maizlish and Handler (2005) discuss the requirements for Title IV Section 404 which they consider to be the core requirements involving the CIO and IT. Maizlish and Handler (2005) note that Section 404 require: statement of management's responsibility for establishing and managing internal controls, an assessment by management of the effectiveness of these internal controls, a statement identifying the framework used, and a statement by the registered public accounting firm describing their audit of the company. Moeller (2013) notes that enhanced financial disclosures are also required. This comes in the form of the SOx Officer Disclosure Sign-off form (Moeller, 2013, p. 25). This form certifies that the employee signing is certifying that the company is SOx compliant.

Rockness and Rockness (2005, pp. 33-34) actually respond directly to the connection of SOx and ethics in their article. They note nine ethical failure areas that relate directly to United States legislation. The ethical failures that can be related back to SOx include: conflicts of interests, prohibited deceit and misrepresentations, fraud of officers and directors of the company, and fraudulent financial reporting. Conflicts of interest are directly connected to SOx Title II Section 206 and Title IV Section 402. The conflict of interest ethics violation could occur if an employee of the company also has a vested interest in another company that can profit by this company's financial transactions. Prohibited deceit and misrepresentations is connected to SOx Title IV Section 406, Title VIII Section 802, and Title IX Section 906. Fraud of officers and directors is directly connected to SOx Title III Section 305 and Title XI Section 1106. Fraudulent financial reporting is directly connected to SOx Title IX Section 903 and Title VIII Section 802. Fraudulent financial reporting would be defined as knowingly providing data to the government which the company or employee knows is wrong, misrepresented, or altered. Thus, it should be very easy to see the direct connection of the SOx Act of 2002 in increasing ethical behavior in companies.

IV. GOVERNANCE AND MANAGEMENT DESIGN

Common Governance Processes and Policies

Brown, Moore, and Tegan (2006) define governance in two primary ways. The first is that governance is to establish and communicate who has the responsibility and authority to make decisions. Second, governance is establishing means to measure plus the policies and mechanisms for control so that the people with the decision rights, responsibility, and authority can and will do their job (Brown, Moore, &Tegan, 2006, p. 3). The topic can also be examined from two perspectives. The first perspective is that of *IT Governance* while the second is that of *Enterprise Governance of IT*. While many older works use IT governance as the terminology, more recent works are focusing more and more on enterprise governance of IT. Haes and Grembergen note this in the title of their article, Moving from IT Governance to Enterprise Governance of IT (Haes & Grembergen, 2009). Haes and Grembergen (2009) also point out that the need to transition to enterprise governance of IT stems from the fact that IT value is directly tied to the business value and strategy.

IT governance can be examined from multiple perspectives. These include: traits, objectives, principals, and enablers. All of these can be categorized under the heading of processes when used as a verb in an action sense. From the perspective of traits, Moeller (2013) notes that good IT governance typically has a control aspect, good coordination, a means of measurement, compliance mechanisms, justification for budget, enterprise wide transparency, and a clear connection to the business strategy. The objectives of IT governance include: strategic alignment, performance management, risk management, and value delivery (Moeller, 2013, p. 30). Particular processes that work to bring about these objectives include: policies and compliance, cohesive security strategy, strategic technology deployment, and education for all stakeholders (Moeller, 2013, p. 30). The five principles of good IT governance are also noted by Moeller from the COBIT standpoint as having an integrated IT framework, stakeholder value drivers, focus on business context, risk management, and performance measurement (Moeller, 2013, p. 69). Finally, the seven enablers required to make IT governance possible include processes, principles/policies, organizational structure, skills/competencies, culture/behavior, service capabilities, and information (Moeller, 2013, p. 72).

Moving now into the realm of enterprise governance of IT, we see that the processes outlined for IT governance are very similar to that of enterprise governance of IT. Wilson (n.d) notes that common enterprise governance processes include:

- Performing conformance management
- Monitoring, measuring, assessing, and adjusting enterprise governance
- Performing configuration management and change control
- Securing the enterprise
- Performing policy management
- Conducting effectiveness and performance management

Brown, Moore, and Tegan (2006) describe these processes in terms of phases (plan, define, enable, and measure governance). Having listed the phases, it is very apparent that many of the same items listed for IT governance also appear as common processes for enterprise governance of IT. A common theme that governance must be tied directly to the business strategy of the organization is prevalent throughout both IT governance and enterprise governance of IT. These processes provide a mechanism for employees to exercise their responsibility and authority of decision rights as well as providing a framework for these employees to operate.

Examples of Strong verses Weak Governance and Key Takeaways

Here, three organizations and their use of information technology (IT) governance are discussed. There is good consistency among the three as far as the main aspects. For instance, Herman, et. al (2011) discussed Saint Luke's Health System and noted that initially there were issues with poor IT governance due to new projects arriving but having no mechanism of control as far as how they get prioritized, budgeted, and how the project gets staffed. What Saint Luke's did well was to establish a good strategic plan for IT governance. This ensured strategic alignment with the overall business, organizational, and IT strategies. A key component of this plan was the establishment of governing boards and committees. This layered use of boards and committees help set priorities and ensure alignment. The layered approach also helps the IT group stay in control as well as maintain the perception of being in control.

The second organization discussed is the IT group at University of California at Berkeley. Spicer and Pirani (2008) noted that there were initial problems with the IT group in the fact that it tried to run like the big, complex academic university itself. The IT group was made up of local IT support trying to establish enterprise level services. Since IT governance was not centralized, there was duplication of investments, lack of flexibility in evolving enterprise services, lack of transparency, and the budget environment was becoming more competitive. To turn the IT group around at UC Berkeley, strategic planning had to be utilized. A series of layered cabinets and committees determined what the IT strategy was and ensured it was aligned with the overall strategies of the university and of the departments. IT governance was then centralized and the cabinet was put in charge of approving all IT investments. Also, it was also uncovered that UC Berkeley did not have the governance processes defined and therefore the funding process as well as the structural roles of the central administration was unclear. Thus, there was no transparency in IT spending. To turn the organization around, UC Berkeley implemented IT governance alignment with campus priorities, transparency in spending, the fostering of partnerships between departments, and a structured IT governance process.

The third organization discussed is the IT group at Queensland University (QU). Pirani and Salaway (2008) point out that a few basics of IT governance were in place there at Queensland University but there was work to be done to improve the situation. First, QU lacked community engagement in IT efforts. Second, consolidation of university-wide IT programs had to be done. Third, strategic planning needed to be implemented. Finally, the financial management of IT spending had to become transparent and centralized. To overcome their problems, QU implemented an IT project portfolio office as well as a three-layer structure to IT governance. Along with that, they implemented strong project management for IT initiatives. These measures helped turn the organization around and get them back on track.

The key tenants and important themes that can be had from the three examples listed above are that IT governance should be centralized and supported at all levels of management. Also, IT governance requires up-front and early strategic planning to ensure that IT initiatives are aligned with the overall business strategies of the organization. Next, IT governance requires good mechanisms and processes to structure the way that projects arrive, get prioritized, and get funded. This generally requires a layered approach in the form of boards and committees. Other key influencers of good IT governance include: good communication of IT project goals, an engaged and educated workforce, transparency of all IT investments (Evans, 2014), strong project coordination, strong leadership support (Evans, 2014), and clearly defined goals. Moeller (2013) spells these out in another way as the enablers that affect IT governance. These include: processes, culture, organizational structure, information, policies, competencies, and service capabilities. Among all of these, it is my own personal opinion that strategic planning and alignment are the most important.

Management Design and Improvement

Milne and Bowles (2009) note that there are five main domains of concern for processes relating to enterprise governance of IT. These are: strategic alignment, value delivery, risk management, resource management, and performance management. Milne and Bowles conducted a survey of three hundred and eighty-nine organizations and reported what they found concerning how good enterprise governance of IT impacts business performance. First, good enterprise governance helps reduce cost, provides for better resource management, helps be compliant with regulations, makes customers happier, provides better data for good decision making, makes the overall business more agile, and improves quality. Those alone are some major general impacts. Some specific performance improvements brought about by good enterprise governance include: improved information management (9% increase), improved business process management (9.1 % increase), improved customer satisfaction (8.8 % increase), and providing more value to products and services (8.9% increase) (Milne & Bowles, 2009, pp. 12-13). Examples of good enterprise governance include using good portfolio management and using a layered board approach for investment decisions. Therefore, good enterprise governance of IT can pay very high dividends when done correctly.

Lajili (2012) gives many examples of enterprise organizational management design. These include management designs such as Transaction Cost Theory (TCT), Agency Theory, Resource Based View/Dynamic Capabilities, Property Rights Theory, and Stakeholder Theory. Lajili (2012) notes that Resource Based View/Dynamic Capabilities Theory is a motivational method that helps ensure alignment of IT investments with business strategy. This is done by aligning the interest of stakeholders as well as presenting a positive work environment for the employees. Enterprise governance is therefore a shared governance method within this framework where participation, equity, ownership, and flexibility are all highly valued and are the norm. The value and impact of using this organizational management design is that it can do

very well in leveraging the organizations capabilities and resources. It also helps to harness the changing capabilities such as investment in specific human capital. The value and effect of utilizing the organizations capabilities and resources probably comes from the fact that the organization is sharing the overall process and responsibility of governance with the employees of the company. Since the employees are involved, they become attached and committed to the governance process and project. With that commitment and involvement comes a determination to make the program work and succeed or the actual reputation of the employee can be tarnished. This type of participation and shared governance by the whole organization is a design method that can bring about more successful project launches and implementations. Utilizing the Resource Based View/Dynamic Capabilities Theory is a means to motivate the employees and stakeholders to help ensure success (Lajili, 2012).

Examples of the Effectiveness and Ineffectiveness of Governance Processes

The common processes of enterprise governance of IT can be implemented and used effectively. If they are not properly implemented, the processes can be ineffective and cause considerable issues. Figure 1.0 below depicts the common processes used and the results of their effective or ineffective use.

Enterprise Governance Process	If Effective	If Ineffective
Conduct Strategic Planning	Strategic plan written, strategy is communicated throughout enterprise	Strategy is not documented, poor communication throughout enterprise, adds to chaos and confusion
Organize Committees and Boards	Layering of approvals is established, prioritization of projects can occur in a logical and strategic manner	No approval chain established, is adhoc, organization that is most powerful wins, organization that is loudest wins
Establish Justification and Funding Approval	Process and standard requirements for justification and approval are established	Standards for justification and approval are not established, inconsistent methods used to justify projects and investments
Perform Conformance Management	A plan to measure and control enterprise governance is established	No plan to measure and control enterprise governance is established therefore governance can go out of control or can become adhoc
Monitor, Measure, Assess, and Adjust	Particular metrics are established, control bounds are established, rules for adjustment are established, control is maintained	No means to control are established so process becomes inconsistent, inefficient, and a balanced scorecard approach cannot be done
Perform Configuration Management and Change Control	The process of change is outlined in detail, the changes approved are prioritized, the configuration of applications and infrastructure are controlled	Changes are done in an adhoc manner, the configuration of applications and infrastructure is not maintained or documented
Secure the Enterprise	IA measure are implemented effectively	IA measures are missed or left out
Perform Policy Management	The proper documentation and maintenance of policies are conducted	Policies are not documented nor maintained hence rules are followed inconsistently within the enterprise
Conduct Effectiveness and Performance Management	The processes of enterprise governance can be measured and improved upon over time	The processes of enterprise governance are not improved over time and can digress

Figure 1.0, Common Governance Processes and Results

Examples of both effective and ineffective enterprise governance processes are abound. For example, if a strategic plan is not written and distributed throughout the enterprise early and up-front, the workforce will not know what is going on and will most likely reject any future projects. Also, if a measurement plan is not fully documented to include the required metrics, then the group monitoring the process will not understand what information is valuable and may allow the process to go out of control.

The core theme throughout all of these common processes is that whatever the project is, it must be aligned with the goals and strategy of the business. Thus, if these common processes are not followed, that alignment with business strategy may be lost. There are many reasons to ensure that good enterprise governance of IT is followed. As mentioned Milne and Bowles (2009) conducted a study on three hundred and eighty-nine organizations and determined that following good enterprise governance helps ensure that there is strategic alignment, value delivery, risk management, resource management, and performance management. Milne and Bowles (2009) also found that organizations that had high maturity levels for enterprise governance also had high performance in their industry. Furthermore, Milne and Bowles (2009) noted that the objectives of IT governance that stood out most frequently included cost reduction, increases in efficiency, utilization of resources, integration, and automation. On the subject of maturity, Milne and Bowles (2009) noted that organizations that were highly mature in enterprise governance were also very focused on the overall objectives and strategy of the business enterprise. To add to the proof, Herman, Scalzi, and Kropf (2011) noted that nearly seventy-five percent of successful IT executives surveyed were active in IT governance executive committees. Herman, Scalzi, and Kropf (2011) also noted that in eighty-seven percent of the respondents, there was a strong correlation between the IT strategic plan and the organization's overall business plan. These are great indicators of the value of good enterprise governance.

As Milne and Bowles (2009) noted, becoming proficient at enterprise governance of IT has great value and provides many benefits. Good enterprise governance helps ensure that projects are aligned with the business strategy. Good enterprise governance also ensures that the decision rights and roles of individuals are presented in great detail and that the framework for these individuals to operate is in place. Whether it is good IT governance or good enterprise governance of IT, the benefits of implementing and using common processes can be very high. On the other hand, not using good common processes for enterprise governance can lead to inefficiencies, chaos, and folks working against the process.

The Impacts of Good Governance

Figures 2.0 through 5.0 (below) are from an empirical study conducted by Lunardi, Becker, and Macada (2009) of one hundred and one Brazilian firms that implemented good enterprise governance of IT. The data set spans samples from the years 2001 to 2007 and crosses 30 different business categories (i.e. banking, airlines, textiles, oil, railroads, etc.). The purpose of their study was to determine if there was a statistically significance indication that enterprise governance of IT was worthwhile and what those impacts might be. Lunardi, Becker, and Macada (2009) studied six performance measures. Three of them were for profitability and three for productivity. The profitability measures used were return of equity (ROE), return on investment (ROI), and profit margin (PM). The productivity measures were asset turnover (AT), operating margin (OM), and operating sales (OS). The measures were measured upon initial implementation of the good IT governance mechanisms and one year later to see the immediate and lasting effects. Lunardi, Becker, and Macada (2009) refer to good IT governance mechanisms as: using a balanced IT scorecard, strategic information systems planning, use of COBIT and ITIL, service level agreements, strategic alignment, information economics, and IT governance maturity model. They used P Value to measure the significance of implementing these processes. Any P Value of less than .05 is considered statistically significant (good). Thus, Figure 2.0 shows how that profitability measure ROE was statistically significant initially and one year later. Figure 3.0 shows that ROI was not significant initially but was one year later. Figure 4.0 was shows that the factors have significance initially and one year later. Finally, for the measures of productivity gain, Figure 5.0 shows that AT was not significant initially but was one year later. OS and OM were not shown to be statistically significant and affected by good IT governance processes.

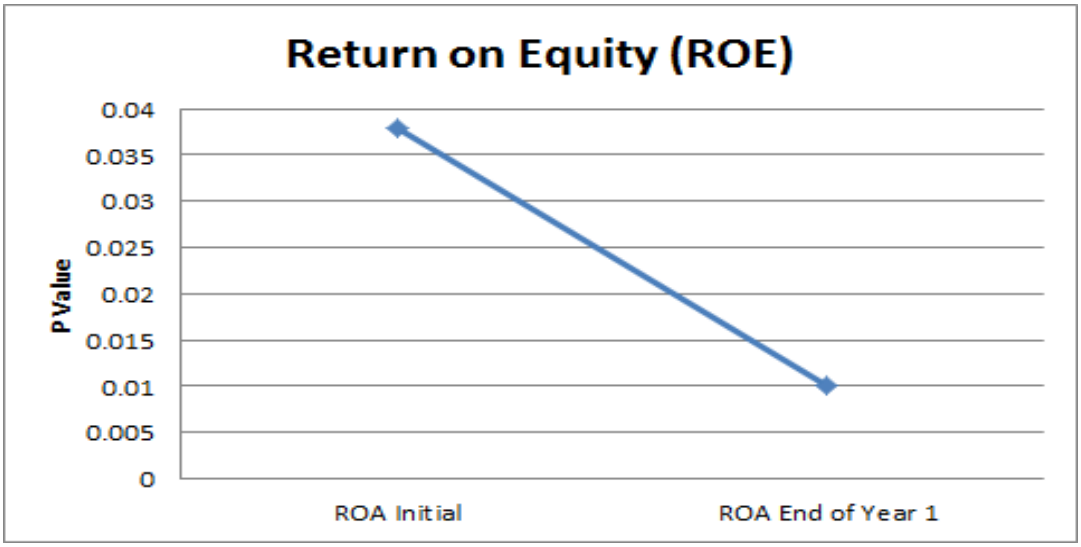

Figure 2.0, Return on Equity

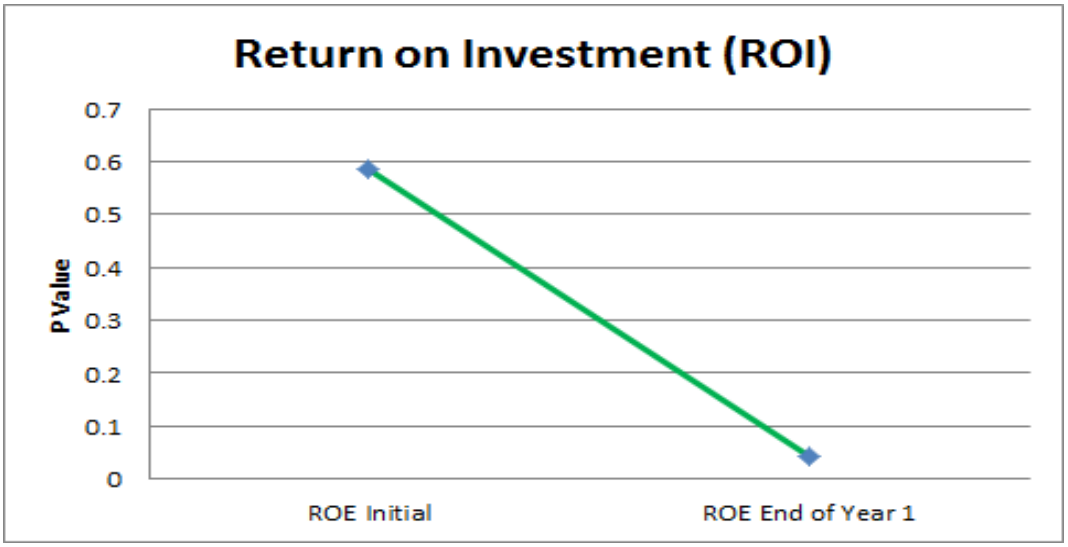

Figure 3.0, Return on Investment

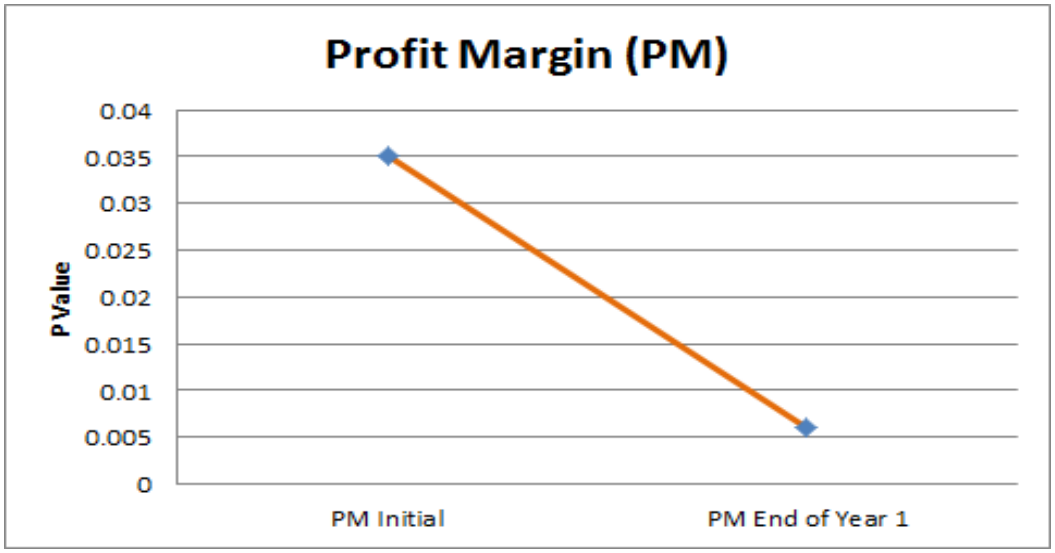

Figure 4.0, Profit Margin

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (125-150), Month: October - December 2014, Available at: www.researchpublish.com

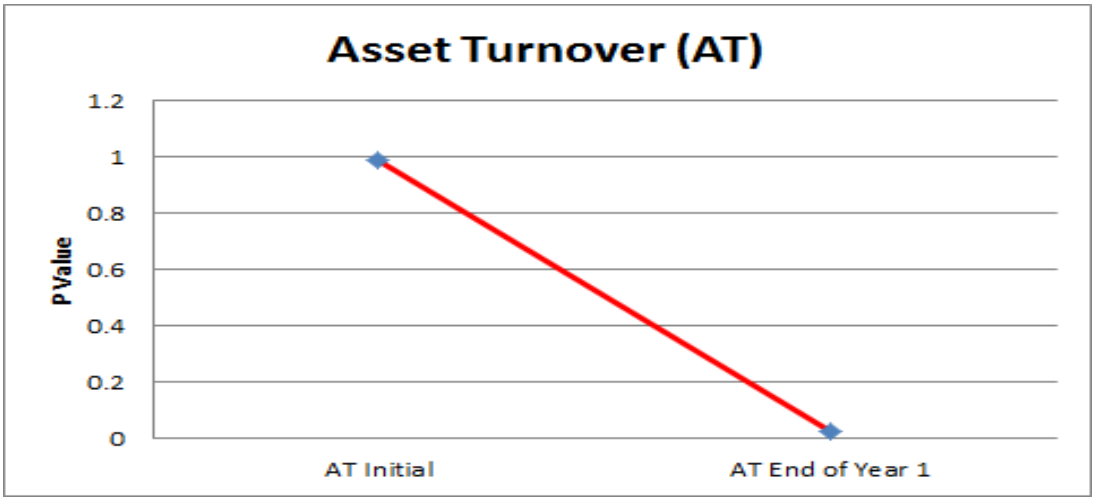

Figure 5.0, Asset Turnover

Cognizant (2013) shows in Figure 6.0 (below) that good enterprise governance of IT can affect business partner satisfaction, value delivery, improved performance/resource management, and quality of IT. The table shows a range for improvements. Business partner satisfaction can improve from fifteen to twenty percent. Value delivery can improve by eight to ten percent. Improved performance can improve from ten to fifteen percent. Finally, the quality of IT can improve up to fifty percent by using good enterprise governance of IT.

Measure	Percent Increase	
	Minimum	Maximum
Increased Business Partner Satisfaction	15	20
Enhanced Value Delivery	8	10
Improved Performance and Resource Management	10	15
Better Quality of IT Output		50

Figure 6.0, Effects of Governance on Business Partner Satisfaction

Finally, Figure 7.0 shows the results of an empirical study conducted on three hundred and eighty-nine global IT firms. In this study, Milne and Bowles (2009) show that an organization maturing in it enterprise governance of IT skills can gain even more over time. Figure 7.0 shows that a firm starting out (low) can expect gains of up to forty-seven percent in performance. Firms at the medium maturity level can expect gains of up to sixty-five percent. Lastly, firms that are at the high maturity level in their enterprise governance of IT capabilities can expect eighty-five percent increases in performance. With these facts in mind, it is great that Herman, Scalzi, and Kropz (2011) found in their study that eighty-seven percent of respondents used strong (high maturity) levels of IT strategic planning for IT governance.

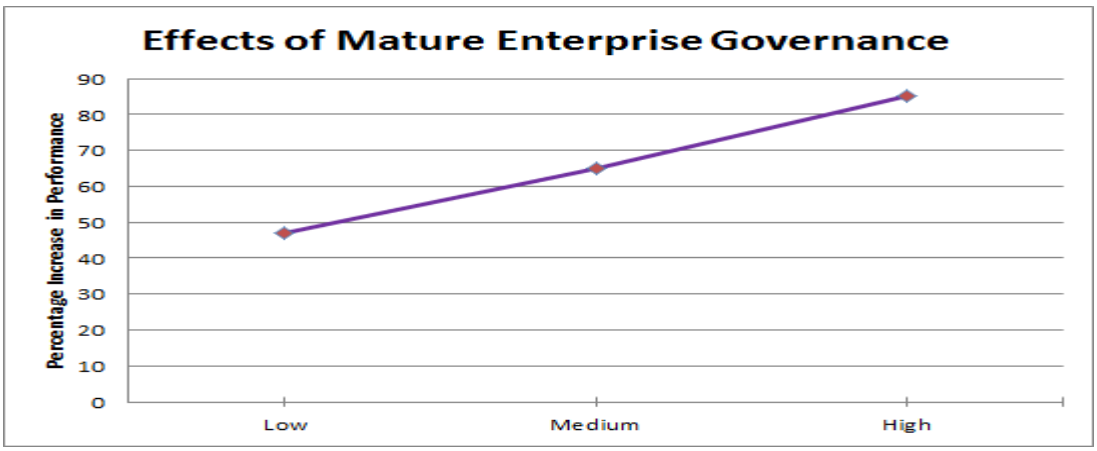

Figure 7.0, Effects of Mature Enterprise Governance

V. POLICY IMPLICATIONS

Sources of Governance Policy

The question of who are the most common sources for enterprise governance of IT policies is a difficult question to answer. It is difficult due to there being many perspectives and multiple contexts in the way the question could be asked. However, having stated that, my own research has consistently found that there are three organizations that supply the best data that I was able to find concerning enterprise governance policies. These three organizations offer multiple articles, standards, frameworks, best practices, or whitepapers on the subject. These three organizations are: IT Governance Institute (ITGI), International Standards Organization (ISO), and Information System Audit and Control Association (ISACA). The following discussion concerns these organizations and their particular contributions to the area of enterprise governance of IT with respect to policies and development. These organizations provide the seminal work in the field provide contributors in the area of enterprise governance of IT policy.

The IT Governance Institute (ITGI) is responsible for publishing and maintaining the Control Objectives for Information and Related Technology (COBIT) framework (Moeller, 2013). The COBIT framework was initially released in 1996 by the ITGI. It was developed initially to both internal and external auditors to use to ensure controls are in place for good IT governance. These controls include good IT governance policy. COBIT provides guidance for assessing these controls and has an emphasis on the utilization of enterprise resources within the IT governance framework. COBIT can be traced back to the Committee of Sponsoring Organizations (COSO) framework which was published by the American Institute of Certified Public Accountants (AICPA) near the year of 1992 (Moeller, 2013, p. 67). Going back even farther, COSO and AICPA can be traced back the ISACA. The overall purpose of the COSO framework was to provide methods for reasonable assurance that the objectives of efficiency and effectiveness were being achieved in financial reporting and enterprise IT governance. The COSO framework has the following as its main parts of the process (Moeller, 2013, p. 65):

1. Understanding and prioritizing risks to enterprise objectives
2. Identifying key controls across the internal control system that address the prioritized risks
3. Identifying information that will persuasively indicate whether the internal control system is operating correctly
4. Develop and implement cost-effective procedures to evaluate persuasive information

Much like COSO, COBIT is made up of key parts that help it become effective with developing and implementing policies for good enterprise governance of IT. COBIT is made up of five principles and seven enablers. The five principles are as follows (Moeller, 2013, p. 69):

1. An Integrated IT Framework
2. Stakeholder Value Drivers
3. Resources Focus on a Business Context
4. Risk Management
5. Performance Measurement

It should be very easy to see the connection between the five principles of COBIT and the four process steps of the COSO framework. Having stated the connection, COBIT was never planned to be a replacement for COSO. Instead, COBIT was intended to be used as a support tool to document the COSO framework. COBIT has seven enablers to achieve this goal. These are (Moeller, 2013, p. 69):

1. Processes
2. Culture, Ethics, Behavior
3. Organizational Structures
4. Information
5. Principles and Policies
6. Skills and Competence
7. Service Capabilities

These seven enables can also be traced back and connected to the COSO framework. The COBIT enablers are more detailed and take the COSO framework process steps to a lower and more mature level. For instance, the COBIT process, principles, and policies enablers can be traced to COSO number 2 and number 4 of the above COSO process steps. This type of linking can be done for each of the COBIT seven enables to the four COSO process steps.

The ISO standards for IT governance include 9001, 27002, and 38500. These can be traced back to the COBIT and COSO frameworks. Since the organization is an international organization, it is located in Geneva, Switzerland (Moeller, 2013). ISO provides a means for an organization to be tested and become certified in an area so as to show levels of competence in that area. ISO focuses on building quality practices that will continually improve IT governance over time to higher levels of maturity. Specifically, the ISO 9000 series is focused on quality management standards whereas ISO 27002 is focused on IT issues relating to security standards. Finally, the ISO 38500 standard is focused on providing a framework to executives and senior management to use to evaluate, direct, and monitor the use of IT in their specific enterprise (Moeller, 2013, p. 119).

As mentioned above in the discussion on COBIT and COSO, much of the makeup of those frameworks can be traced back to the work of ISACA. ISACA was originally more focused on providing tools for auditors to use. In fact, ISACA certifies IT auditors with its Certified IT Auditor (CISA) program. This CISA certification is granted by examination and professional designation from ISACA (Moeller, 2013, p. 68). ISACA also has the Certified Information Systems Manager (CISM) program which is mainly for IT security managers. These auditors do both internal and external auditing for enterprises. Thus, ISACA is the seminal organization dating back before both the COSO and COBIT frameworks.

The organizations or authors who play a contributing role to the area of IT governance policy include: IBM, National Computing Centre (NCC), Haes and Grembergen, and finally, Milne and Bowles. Each organization or author has done works that have either directly been implemented into ISACA, ISO, or ITGI documentation or have published works that add to the body of knowledge. The following is a discussion of their contributions and linkages to more seminal organizations in the field of IT governance policy.

The IBM web site offers great data and many articles on the subject of enterprise governance policy. One such article is that of Brown, Moore, & Tegan (2006). Their article focuses on the governance of an organization using a service oriented architecture (SOA) approach. The value of the article is to explain the benefits of using a SOA and discuss how to implement it correctly so that these benefits can be achieved. The premise of the authors is that it takes good IT governance to implement and utilize SOA correctly. Thus the authors present an IT governance model for SOA implementation. Their model is made up of four major steps which are: assemble, deploy, manage, and model. These steps can be traced back to COBIT and COSO frameworks.

The NCC developed an excellent best practice whitepaper which can be found at the ISACA web site. The whitepaper is entitle, *IT governance: Developing a Successfully Governance Strategy* (National Computing Centre, 2005). It contains thirteen excellent chapters on the subject of IT governance. The chapters cover the topics of: business case development, performance measurement, roadmap development, communication of strategy, capability maturity, risk, suppliers, IT auditing, IT security, statutory IT governance, architecture, IT investment management, and success factors. These chapters can be traced back to ISACA, ISO, and ITGI frameworks.

Haes and Grembergen (2009) wrote an excellent article that was published in the *ISACA Journal.* The article discusses how an organization can move from thinking in terms of IT governance to broader thinking in terms of enterprise governance of IT. By doing so, an organization will realize the focus of IT should be on the enterprise business strategy and improving the enterprise. Thus, all IT investments should flow into an enterprise business strategy and provide value in the form of efficiency, effectiveness, profit, or stakeholder value. This concept of thinking can be directly traced to ISACA and COBIT.

Milne and Bowles wrote an excellent empirical study as a best practice for the IT Process Institute. This empirical study was entitled, *How IT Governance Drives Improved Performance* (Milne & Bowles, 2009). The whitepaper was published in the ISACA organization web site. The empirical study researched three hundred and eighty-nine global IT organizations and revealed that there are basically three levels of maturity when it comes to IT governance. The study gives empirical evidence to the performance improvement that can be expected for each of the three levels of maturity. It assessed the maturity using sixty-six best practices in five major IT governance domains. These five domains are: value

delivery, risk management, resource management, performance management, and strategic alignment. All of these have previously been mentioned and can be traced back to the ISO, COBIT, or COSO standards for IT governance.

To reiterate, the question of who are the seminal organizations for IT governance policy is a hard question to answer. Nonetheless, my research found that there were three organizations where most (if not all) modern IT governance thinking can be traced. These are: IT Governance Institute (ITGI), International Standards Organization (ISO), and Information System Audit and Control Association (ISACA). These organizations offer standards and frameworks such as COSO and COBIT to help govern the IT enterprise. Further, my research found that there were many supporting and contributing organizations or authors. Four organizations or authors that stand out include: IBM, National Computing Centre (NCC), Haes and Grembergen, and finally, Milne and Bowles. Each of these was discussed in detail and their linkages were traced to the seminal organizations for enterprise governance of IT and the policies thereof.

Key Points of Policy and Impacts

Evans discusses the policy development process as *strategy implementation* (2014, pp. 228-230). The key components of a successful policy development revolve around three main areas according to Evans (2014). These are senior management, middle management, and implementation teams. These three groups have to accomplish four overall tasks for a policy to be successfully developed and implemented. These four overall tasks are referred to by Evans (2014) as: plan, do, study, and act. Much like Evans (2014), MN IT Services (2012) discusses the process in four tasks but in slightly more relevant terminology. MN IT Services (2012) refers to the four tasks as: aligning goals, managing risks, optimizing resources, and exploiting the benefits of the policy implementation. Yet even other authors refer to the four tasks as: IT value alignment, risk management, performance measures, and accountability. Although worded slightly different, each author has very similar definitions for the four tasks of policy development and implementation. For this discussion, the Evans (2014) terminology will be used but augmented with other terminology to provide clarity. Thus, plan will mean alignment, do will mean managing risk, study will mean measuring performance, and, finally, act will mean being held accountable for the next step.

Each of the four tasks is handled at various levels within an enterprise or organization. For instance, Evans (2014) points out that planning and alignment, which involves setting goals for this phase and reviewing the results for the next iteration, is generally done by top management. Middle management generally does the setting of accountabilities and managing of risks which involves goals and measures. Finally, the implementation team is responsible for the doing and acting which involve measuring performance and preparing the results for management review. Then, senior management starts the whole process off again with the next iteration. This process has major effects on the enterprise. For example, middle management of the enterprise is affected in the sense that they are held responsible for setting the vision and objectives for the policy development. Top management must also communicate these visions and objectives. Middle management is affected in the sense that they are held responsible for setting the strategy and utilizing the resources correctly. Middle management must get progressively more detailed in the planning and must provide a clear link to the common goals from top management (Evans, 2014). The implementation team is affected due to the fact that they are held responsible for action and schedule. The implementation team which is at the lowest level is affected in the sense that they must interpret what middle management has planned and they must measure their own work to show success (Evans, 2014). These measurements are then communicated up the chain as feedback to senior management who decides the next step. The emphasis is on improvement. The whole process is referred to by Evans (2014, p. 228) as *hosin planning*.

The overall effect of using this method is continual feedback with an emphasis on performance improvement over time. The measures provide a mechanism for this feedback and are checkpoints to ensure both individual success and enterprise-wide success (Evans, 2014). The process starts with senior management but involves all levels throughout the organization.

Good and Bad Policies

There are policies and there are regulations. Here, policies are defined as principles used as a guide to achieve a desired outcome. Regulations, on the other hand, are defined here as those rules that are statutory and required by law. These are two distinct and separate subjects. In this article, only policy is covered. Having stated that, an example of a good policy for information technology (IT) governance is the policy to make sure that all systems within an enterprise are reviewed

for information assurance and security prior to implementation. The reasoning for this should be apparent but is to make every effort to keep the data that a company has (both proprietary and private) out of the hands of competing companies. Competing companies could use the data to gain competitive advantage or to offset rivalry with competitors as mentioned by Porter (HBR, 2013, pp. 46-47) in his discussion of the five forces that shape competition. Any organization should not want their data being given out to competitors without them knowing. That would be bad business.

Examples of bad policies for IT governance are: limiting competition between suppliers, the policy to use only in-house developed software instead of commercially available software, and not having a good deployment plan in place for implementation of IT projects. Sharma, Stone, and Ekinci (2009) discuss in their research how an organization had hired two companies to provide software for a major project. One software supplier chose to buy commercially developed software products while the other chose to develop their own software in-house and deliver it to the customer organization. This was the policy of the software provider. Later, problems surfaced in the form of communications. The software provider that did the development in-house was not inviting the customer to internal meetings and did not keep the customer abreast of issues with the software as it was developed. This left the customer organization in the dark and at risk as far as schedule is concerned.

Another bad policy for IT governance pertains to Toyota's policy on supplier competition Rajan and Zingales (1998) discuss on how it is Toyota's policy to down-select to only two suppliers and how this gives the suppliers bargaining power. The power comes from the fact that Toyota does not guarantee either of the two down-selected companies any business. So, one company can gain power over the other supplier if they chose to invest more and provide Toyota with something more desirable. Thus, one supplier can gain advantage over the other and Toyota could be left with only one final supplier if the other choses to pull out or go bankrupt. Therefore, although this policy might look good to Toyota, it could come back to haunt them.

In my opinion, the policy that makes the biggest impact is the policy to have policies in place before any IT project that is approved is implemented. Evans (2014, pp. 228-229) discusses the concept known as *hosin planning*. In other words, it is the policy to have the policies written and in place prior to the need. It is the policy on how to deploy policies and it can be critical to the success of IT project implementation and use. Having the policies in place, up-front, allow the employees to know what is expected before they present a new IT project. This causes the employees to present better packages for review and justification.

VI. CONNECTION BETWEEN ETHICAL BEHAVIOR AND SARBANES-OXLEY

Key Points of Ethical Behavior

Reynolds (2012, p. 3) states that ethics are the set of beliefs about right and wrong behaviors that are found in a society. That is to say that to be ethical means that one would be practicing norms that are generally accepted by a particular society. Of course, these norms change and vary from society to society and are affected by culture, values, morals, laws, and religion, to name a few. There are many good reasons for companies to promote ethics and act responsibly. These include: gaining goodwill, perpetuating consistency, fostering good business practices, positioning to be legal, and avoiding unfavorable comments and perceptions from the public (Reynolds, 2012). To achieve these benefits a corporation or enterprise needs to practice some key ethical conduct. A few very key examples of ethical conduct that has both impacts and effects on the enterprise are: appointing a corporate ethics officer, holding board members to high ethical standards, establishing a corporate code of ethics, and requiring employees to take ethics training (Reynolds, 2012). Appointing a corporate ethics officer impacts the company due to the fact that the company now has one person to rely on to assemble and maintain all the necessary ethics materials and be the champion for the ethics program throughout the company. Holding board members to high ethical standards is also a necessity and can have great impacts to the company if not done. In other words, any behavior that a corporate executive exhibits that could be viewed as unethical would tarnish the perception of the company and could even lower stock prices. Establishing a corporate code of ethics has impacts in that it sets a standard that flows from the top to the bottom for expectations of conduct by all employees in the company. Lastly, ethics training is very important and can have major impacts to a company if it is not done. For instance, if employees have no ethics training and are not exposed to the corporate expectations for conduct, they are free to follow their own ethics and as I pointed out, ethics can vary from person to person depending on many factors.

Reynolds (2012, p. 387) notes that ethics has a direct correlation to profitability for corporations. Thus, ethics as a whole is tremendously important to a company meeting their sales, profit, and performance goals. Reynolds (2012, p. 10) also points out that the one hundred most ethical companies in the world have very consistent stock performance. So many times the perception of a company is tied directly to the reputation of a board member. With that relationship and correlation stated, holding corporate board members can have a direct impact on the profitability of the company as well as the stock price. Therefore, ethics is very important and has many impacts. Two more key ethics points are also very important and have large impacts. For instance, having a corporate code of conduct and holding employee training on this code of conduct for ethics affects many things. LRN (2006) notes in a study they presented that this code of conduct and training helps approximately seventy-six percent of employees understand the code better. Also, seventy-three percent of the employees believe it makes the company a better place to work. Sixty-two percent of the employees believe that it helps alter the behavior and decisions made within the company. Finally, forty-six percent of the employees believe that people know the rules but do not always follow them. Thus, having a policy and code of conduct is one thing, but compliance to the policies is also very important. These three small changes of key points relating to ethics that I mentioned above have the most impact, in my opinion.

Ethics is important in companies for many reasons. The lack of ethics can cause the perception of the company and its employees to dwindle which can affect stock prices and profit. It can also affect the life of a company. Putting good ethics practices in place in an organization therefore can pay high dividends and should be done from the highest board member down to the lowest worker. Ethics is important. Reynolds (2012, p. 3) describes ethics as a set of beliefs about right and wrong behaviors that are found in a society. Being ethical therefore means that a person would be practicing the norms that are generally accepted by a particular society. Unfortunately, norms can change from society to society and are often influenced by culture, values, morals, laws, and religion. Noting this, it is important to keep these facts in mind as a company moves from one country or region to another. This variation in norms can affect the image of the company. So, it is important to maintain a code of conduct for ethics from location to location. LRN (2006) notes that a code of conduct for ethics and training in ethics helps approximately seventy-six percent of employees understand the code better. If the expectations are understood better, then they can be executed better. Even more so, seventy-three percent of the employees believe a code of conduct for ethics makes the company a better place to work. Making the company a better place to work is imperative to surviving the long term. Sixty-two percent of the employees believe that a code of conduct for ethics helps alter the behavior and decisions made within the organization. Making better decisions can make or break a company. Thus, ethics is important and has many benefits.

Reynolds (2012, p. 10) notes that one hundred of the most ethical companies in the world were studied and found to have very good stock performance. Often the image of a company is directly tied to the perception of its board members. Thus, not holding corporate board members accountable to a higher standard of ethics can have a direct impact on the profitability of the company, profit margin, and the stock price. With that said, it is very important for the company, its board members, and its employees to have a good image from the standpoint of ethics and integrity. Violating ethical norms can bring about devastating consequences to organizations and actually drive them out of business if the ethics failure is not remediated.

Dietz and Gillespie (2012) note that there is a clear linkage between trust and ethics. If an organization cannot be trusted, it is typically also not seen as ethical. They point out that past surveys show that customers, investors, and other stakeholders are becoming increasingly more skeptical of the ethics of companies in the business world. In fact, Dietz and Gillespie (2012) point out that surveys show that trust almost bottomed out after the financial crisis that happened in the 2007-2008 timeframe. Thus, it is important for companies to be perceived as trustworthy and ethical for them to attract these skeptical customers and stakeholders. Sometimes building trust based on ethical behavior can take time and so companies must be willing to do the right thing over the long haul. Any mishaps or ethics violations along the way can totally destroy all the trust built up to that point. Dietz and Gillespie (2012) note that ethical conduct has as its central theme items such as integrity, actions matching words, fulfilling promises, making a good effort, and showing genuine concern for stakeholders.

The level of confidence one has that an organization can be trusted and relied upon often ties directly to the organization's perception of ethics. Thus, to correct for mishaps or violations of ethics, it is often necessary to work to rebuild the level of trust a stakeholder has in an organization. Dietz and Gillespie (2012) recommend that organizations demonstrate their trustworthiness in ways involving technical competence, products and services, and through exhibiting positive motivations and concerns. The first overall step in this process is to create regulation or policy that must be accomplished

to repair the ethical image. The second is to work to fully demonstrate that the organization can actually still be trusted. This process of trust repair and perception rebuild is made up of four steps. These are:

1. Perform an immediate verbal response which is further backed up by actions within the company
2. Conduct a study to diagnose the system or policy failures that allowed the mishap to happen
3. Bring about reform to intervene. In other words, verbal apologies and payouts where necessary. Generate policy or regulation to intervene. Then fully implement any necessary reformations found
4. Evaluate the whole system at all levels

Following these steps can help rebuild trust in a company and can therefore improve and repair the image of an organization over time (Dietz and Gillespie, 2012).

Relationship between Policy and Ethics

This is a subject very near and dear to me on a personal level since I personally work in the Governance Group within a CIO group. In my opinion, the very most important part of the governance process that has a direct tie to ethics is the process of information technology (IT) investment presentation, justification, and approval. This process is discussed below and brings about the required accountability, transparency, and compliance that are now required by law.

Maizlish and Handler (2005, p. 9) note that the primary reason for the need for an additional law (Sarbanes-Oxley Act) is due to poor accounting practices, lack of transparency, and lack of traceability of corporate behaviors by companies such as Enron. In other words, poor ethical behavior is the cause for additional law. Thus, the direct tie from governance to ethics is assuring accountability, transparency, and compliance. With that said, having an excellent and fully documented governance process that fully outlines the steps necessary to present, justify, and gain approval of an IT project is totally essential to both keeping folks ethical and practicing good IT governance. Moeller (2013, p. 81) further points out that governance is almost always the responsibility of the board of directors under the leadership of an executive such as the Chief Executive Officer (CEO). Moeller (2013) also points out that governance and management involves being very efficient in the use of resources, people, processes, and practices necessary for an IT project. The overall objective of the IT governance process is to ensure that the IT project being proposed aligns with corporate business strategy and is executed in a way that provides transparency and accountability.

In his discussion on causes of concern for IT professionals, Reynolds (2012, pp. 41-42) discusses both IT governance and transparency in the same discussion. Reynolds (2012, p. 42) defines transparency as, *the attempt to reveal and clarify information or processes that were previously hidden or unclear*. This definition, in context with the discussion of causes of concern for professionals that deal with IT, further helps to prove my point that governance and ethics is directly linked at accountability, transparency, and compliance. This also happens to be the place where IT project justification is done in the governance process. Thus, a good governance process that has at its core an excellent IT project justification process ensures both good ethics and good governance. Good governance helps ensure compliance.

The Need for Auditing

Reynolds (2012) notes that as early as 1972, the SEC recommended that publicly held corporations should establish the role of an auditing committee. Initially, this auditing committee was to augment the board of directors of the company by providing assistance in the responsibility of oversight. The main purpose of the auditing committee was to: provide quality and integrity, require compliance, provide independence in auditing, and perform as the company's internal auditing group. The auditing committee were not initially required to be experts in finding and investigating financial impropriety but were really there to provide advice on how to better develop policies and procedures to satisfy Generally Accepted Accounting Practices (GAAP).

Moeller (2013, p. 9) points to a more recent cause for even more regulation concerning the necessity for audits. This is the famous Enron financial impropriety that spurred SOx which happened in 2002. The act has many parts and sections with some being more important to information technology (IT) than others. The sections that are of particular interest to auditing for IT are: Section 108 (Auditing Standards), Section 301 (Audit Committee Independence), and finally Section 404 (Internal Control Reports). Section 404 has been a source of major work efforts for corporations trying to establish compliance to SOx and is said to be the most important for IT (Moeller, 2013). It is made up of the internal audit controls necessary for compliance checking. Thus, auditing is a necessity that was brought upon initially by the financial misdeeds of companies and is now a highly regulated necessity.

Auditing is an essential part of any system where control measures are put in place. In layman's terms, it is the measuring of compliance to a set of rules or policies. Reynolds (2012) specifically defines auditing as the performance of five major tasks. These are:

1. The determination if internal control systems and controls are adequate
2. Verifying the existence of company assets and maintaining the safeguards to ensure their proper protection
3. Insuring that the proper policies and procedures, laws, and practices are available and followed
4. Measuring the level of compliance that the organization has to its own policies and procedures
5. Evaluating the level of adequacy and compliance with said policies, procedures, laws, and practices. Also to evaluate the reliability of the information used in the evaluations

The performance of these five major tasks make up the verb, auditing. Auditing is a verb that shows action and the tasks are the actions that are essential to success.

Moeller (2013) points out that there are two overall types of auditing that come from the new regulations outlined in the previous section. These are financial audits and information technology (IT) audits. The GAO (2009) points out that IT audits also include the auditing of information and information systems. NIST (2010), NIST (2013), as well as Johnson and Toth (2007) point out that IT audits also include the auditing of information security. Thus, although there are only two overall categories, there are many aspects of auditing with respect to IT. This section will discuss all the types of auditing listed: financial, information technology, information systems, and information security.

A very essential part of auditing is the idea or concept of independence. Moeller (2013) notes that auditors have historically performed as separate entities from the main organization. This brings about the idea of fairness and the feeling of being unbiased that is so valuable to government organizations that may be looking or investigating a company. Often, the role of an auditor is outsourced by the company. Outsourcing of auditing has been happening since the late 1980s (Moeller, 2013, p. 19). In fact, SOx actually prohibits many functions of public accounting firms so that they would not be able to also perform the role of auditor. Moeller (2013) lists these prohibited functions as: financial information systems design, book-keeping, financial statements, management of human resources, and actuary services. Thus, the government is very serious about the concept of auditor independence.

The two primary bodies that make up the field of auditing are the auditing committee and the internal auditing team (Reynolds, 2012, p. 64). Reynolds (2012) further points out that the overall goal of the auditing committee as well as the members of the internal auditing team is to ensure that both IT organizations and IT users are in compliance to the policies and procedures of the company as well as laws and regulations. Indeed, this is the overall value of the role of auditing – to keep the company out of hot water and stay in compliance.

Moeller (2013) points out that Section 202 of SOx, Title 1 specifies that the auditing committee is there to approve all audit and non-audit services before they happen. The auditing committee adds the formality to auditing that is necessary to satisfy government regulation. Audit committee members are actually liable for the decisions they make and can be face criminal charges if they do not perform within legal boundaries. Some non-audit services that must be approved by the auditing committee include: checking that value of services does not exceed percent of total audit fee, ensuring that all services are recognized upon initiation, and all services are approved prior to an audit. The requirements for the makeup of the audit committee are that they should be independent directors with no connection to the management of the corporation. Typically, the committee is made up of five or six members to support a board ranging in size from twelve to sixteen board members. Guest can be invited but they are not allowed to be voting members of the auditing committee (Moeller, 2013, p. 372). The audit committee is also charged with the responsibility of forming and running the internal auditing function as well as hiring the auditors (Moeller, 2013, p. 373).

The role of internal auditors is defined by SOx Section 404, as well. They are responsible for putting the internal controls in place within the company and verifying compliance to these controls. Moeller (2013, p. 17) list the major responsibilities of internal auditors. These are: focus on internal controls, eliminate audit procedures that are not necessary, and make the audit scalable to fit the specific complexity of the company being audited. If an internal auditor finds that there are items or people that inhibit their ability to perform the audit, Moeller (2013) points out SOx, Section 404, AS5 requires an external auditor to be called and perform the evaluation. The internal auditor team generally follows a six step process as indicated below (Moeller, 2013, pp. 326-327):

1. Schedule the audit
2. Assign the auditors
3. Perform preliminary audit assessment
4. Document the processes for the section being audited
5. Evaluate the internal control system
6. Prepare the results and reports

Following these steps helps internal auditors provide consistent and credible audits that are of value to the auditing committee and any subsequent government auditing investigations.

The major parts of a financial audit cover the areas of revenue cycle, direct expenditures, indirect expenditures, payroll, inventory, fixed assets, and the general controls of IT cycle (Moeller, 2013, p. 15). Of particular interest to IT are the general controls of IT cycle. This includes many aspects of an IT project and overlaps with the process of IT governance. The particular areas to be audited for the general controls of IT cycle include: strategic alignment to business strategy, value delivery, risk management, resource management, and performance management (Moeller, 2013, p. 330). All of these items make up the internal audit of IT and are the focus of IT governance, as well. Thus, auditing plays a major role in any good IT governance process.

GAO (2009) outlines the requirements for internal audits concerning various information types and the information systems that use this information. The Federal Information Controls Audit Manual (FISCAM) is considered the go-by reference for information and information system audits. The overall methodology of the FISCAM is to perform a top-down audit to ensure the controls are in place. The main concerns for this type of audit are that controls are in place to secure information, limit access to the information, protect the information, provide for configuration management of the information, segregate duties, and provide for a contingency plan. All this is put in place to ensure that the information is: complete, accurate, valid, confidential, and available.

NIST (2010), NIST (2013), and Johnson and Toth (2007) all cover in great detail the specific area of internal auditing for information security. Both NIST documents are in place as part of the Federal Information Security Management Act (FISMA). All of these documents were put in place to ensure that sufficient controls are in place to verify that the information stored on computer systems is secure and safe from hackers and such like. They exist to make sure that companies and organizations perform due diligence in safeguarding information and providing privacy for individual's data. Their process includes the use of penetration tests and the generation of reports that outline the level of security of the information.

The use of auditing committees and internal auditors can pay high dividends if done correctly. The following outlines the hypothesis concerning the impact of auditing and the compliance thereof. It is hypothesized that establishing controls, verifying compliance, and performing audits will improve the overall performance of an organization in the form of increased efficiency, higher profit margins, and increased sales. The reasoning behind this hypothesis is simple. The primary hypothesis will be true because implementing good controls and auditing practices is mandated by the government. If any violations occur, there will most likely be very stiff financial penalties and perhaps even jail time. The less financial penalties a company has, the more likely they are to increase profit share and performance. Having these controls in place also makes a company more efficient since the controls add to the repeatability of the process. This repeatable process can come in handy and provide better overall performance in efficiency to the corporation. Auditing is an important part of IT governance as well as being required by regulation. This, auditing is important and should be done correctly. The lack of good auditing practices can have the negative effect which is not what a company that is trying to grow and be successful should be doing.

Example Impacts of Non-Ethical Behavior

Siemens: In the month of November of 2006, the German company, Siemens, was found to have been performing many unethical practices concerning false companies, false contracts, bake bills, and shell firms. This was done so that the company could come up with funds to pay bribes and make pay-offs to win contracts for the company. Officials and managers of Siemens were blatantly ignoring company policy and legal regulation. Senior managers even used removable Post-it notes to authorize and approve the payment to these false companies and entities.

In the eyes of the German public, Siemens was totally shamed and untrusted for committing these unethical behaviors. It was thought of as a public humiliation for the German people. Influential groups questioned HP's board on it competency to even handle this total failure in ethics. Siemens held their ground and did not react at first. But, their final and belated reaction was later found to be highly effective. It has even been praised as an excellent response to unethical behavior and has since been studied by organizations as a model on how to handle these type events.

The method of remediation that Siemens used was to immediately play down the affair by underestimating the total funds that were expended in this mishap. Next, all major officers of the company denied any involvement in knowing about the misconduct. Then Siemens addressed the stockholders and cited "deep distress that the compliance regime had not prevented the alleged misdeeds" (Dietz & Gillespie, 2012, p. 8). Many viewed this first set of responses as incompetence. Then Siemens conducted a diagnosis through four investigations. After the diagnosis, Siemens put in place a new system to detect and prevent this from ever happening again. Since the investigation was very in-depth, it convinced most skeptics. Next, Siemens appointed a new board member. The new board member was a co-founder of Transparency International so this helped improve Siemens image. Then, the new strict rules were implemented and launched within the company. All of this was used to drive a culture change at Siemens.

As part of a continual effort, Siemens reviewed millions of bank account statements, documents, and bank transactions all the way through 2008. Their new system is praised by many for its ability to identify unacceptable practices and prevent events such as the event described above from ever happening again. The scandal ended up costing Siemens much but trust was re-established and the perception of Siemens being ethical was regained.

Hewlett-Packard: In 2005, a person was hired as the new CEO of Hewlett-Packard (HP) (Reynolds, 2012, pp. 1-2). This person did a great job from 2005 to 2009 in doubling the stock price and growing revenues by forty percent. The new CEO accomplished this by doing many very common things like: cutting costs, reducing jobs, and acquiring many technology based firms. It would seem that all was going great but in 2010 the new CEO was accused of sexual harassment. The person doing the accusing was a female who often spent much time with the new CEO over the course of two years. It also happened to be a contractor who worked for HP. She alleged that the new CEO made sexual advances toward her and she refused. Then shortly thereafter, her work with HP was canceled by HP. She further accused HP of stopping the work due to her not accepting the CEO's sexual advances.

An investigation was held in the matter and it uncovered some very unethical behaviors on the part of the new CEO. One such unethical behavior was the fact that he was making payments directly to the woman through reimbursements for expense reports. The investigation was not, however, able to substantiate any sexual misconduct on the part of the CEO. Unfortunately, this did not matter in the eyes of public opinion. HP was seen as behaving badly due to the CEO's actions and profound lack of judgment. Thus, HP was forced to remediate the situation.

HP attempted to remediate the situation by first calling for the new CEO to resign, which he did not do until after many discussions with HP board members. The new CEO then moved directly to a job with a partner of HP (Oracle). This was seen as a violation of a nondisclosure agreement made between HP and the CEO. HP filed a lawsuit to try to keep the CEO from going to Oracle. An agreement was finally reached where the CEO could move to Oracle but had to give up all HP stock and not disclose any HP data to Oracle. Thus, the method of remediation of the ethics violation of the CEO was to remove the CEO from HP and hope to repair the company's image.

This section laid out the definition of ethics and why it is valuable. Remediation processes were discussed by first showing the linkage between trust and ethics and then describing the detailed steps involved in repairing trust if a breach happens. Then two case studies were highlighted and their remediation methods were described. Siemens was able to remediate their massive breach of trust by performing a set of steps to help rebuild their image. Siemens first downplayed the mishap and then investigated it heavily. After the investigation, a system was developed to help identify potential violations and prevent them from happening. To help with the launch of the system, Siemens hired a person who was known or perceived to be highly ethical. These steps, as well as continuing to use the system well after the mishap, helped Siemens regain trust and build a better ethical image. HP was able to remediate its breach of ethics by separating the CEO from the company and then work directly on re-establishing the image of trust and ethics that the company had just before the incident. In both cases, trust was able to be rebuilt and an ethical image was re-established. It goes without saying that it is better to not have ethical mishaps but, if they do happen, it is nice to know there are methods that can be used to help rebuild trust and improve the company image.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (125-150), Month: October - December 2014, Available at: www.researchpublish.com

VII. SARBANES-OXLEY ACT

The Need for SOx

Throughout the existence of man-kind, there have been multiple examples of the evilness that men are capable of committing. We have heard of the many stories in the Holy Bible going back to the beginnings of history in chapter four of Genesis with the story of Cain slaying Abel. Cain was jealous of Abel and the favor that God showed toward him (Bible, 2000). Later in Genesis we see the story of Joseph and his brothers who were all the sons of Jacob. Joseph was the favored son of Jacob and Joseph's brothers despised him for it. They through him in a pit and sold him in Egypt (Bible, 2000). The basis for both the actions of Cain as well as the actions of Joseph's brothers was jealousy. Jealousy can present itself in many ways. Jealousy can be in the form of killing a fellow man because you want his wife, his goods, his money, or his power. Jealousy can also be in the form of trying to have more or get more than your fellow man. And still yet, jealousy can also be in the form of seeing something your fellow man has and wanting to take it from him. So, jealousy is the main driver of envy and greed which can drive man to do unthinkable things.

The discussion of how all this plays into business can now be made since the discussion of jealousy, envy, and greed being di a primary driving force for mankind has been made. The basic premise is that jealousy, envy, and greed are all evil. Man will either be good or he will be evil. Those that will be good will be good regardless of the situation. Those that will do evil will do evil when opportunity knocks and allows them to get some gain they would not otherwise have gotten. This includes all levels of management from the lowest level to the highest within a corporation. This also includes the workers in a corporation. Those that will commit evil have the propensity to seek ways to make even more gain than would be legal. The greater the opportunity for gain is the greater the propensity to commit evil will be. Thus, those who will commit evil will also disregard laws and regulations if they know there is no great penalty for violating these laws. There must therefore be compliance measures and penalties along with laws if we are to thwart those that would commit evil and perform unethical business practices.

This section discusses the propensity of man to commit unethical business practices if they will not be caught. It then discusses the many examples of business misconduct that have happened in recent time. Then, the laws and sub-parts of these laws that deal with unethical business conduct and the punishment thereof will be discussed. Finally, an opinion will be presented on if government should be involved in businesses and how should government be involved. The section wraps up with concluding remarks.

Examples of Known Misconduct for SOx to Find and Halt

Rockness and Rockness (2005) list thirteen major corporations that have committed business or ethics misconduct and that have been charged with financial irregularities. These include:

- Sunbeam, 1996-1997, $60 million
- Waste Management, 1997, $1.7 billion
- Xerox, 1997-2000, $1.5 billion
- Adelphia Communications, 2001, $3.1 billion
- WorldCom/MCI, 2002, $3.8 billion
- Anderson, 2002
- Global Crossing, 2002
- Tyco, 2002, $600 million
- Imclone Systems, 2002
- Healthsouth, 2003, $4.2 billion
- Ahold NV, 2003, 900 million euros
- Enron, over $1 billion

All of these organizations committed some sort of financial or unethical conduct to somehow make some financial gain that would not have been achievable had they followed the laws of the land. Each of them had a set of workers, a

management structure, and corporate executives who were at the helm. Still, each company committed business misconduct to the tune of millions or billions of dollars. Why is this? The answer ties directly to the concept of evil works connected to jealousy, envy, or greed. The parties who would have gained from these financial misconducts were committing evil in order to get something from their fellow man that they would not have otherwise been able to get. This leads to and is the basis for the need for not only laws and regulations but also severe penalties for misconduct.

All of the companies outlined above were also given some sort of penalty for their misconduct. These penalties ranged from executives resigning, civil court settlements, filing of bankruptcy, executives being charged with fraud, jail sentences, convictions for obstruction of justice, and indictments for falsifying records (Rockness & Rockness, 2005). The types of crimes committed by these companies included many things. Sunbeam, for example, underestimated their inventory value and gave inaccurate financial data to establish false reserves and improve income. WorldCom/MCI reported line rental expenses as capital lease assets as well as not recording loans to executives. Anderson destroyed financial documentation that would have been used against them in SEC investigations. Tyco gave loans that were not authorized or recorded to senior executives. Ahold-NV overestimated its income and gained from discounts prior to the sale of goods. Enron, the most well-known of the modern bad companies, gave fraudulent financial reports which overestimated their income. This hid many of the losses that Enron had actually incurred and was not released as knowledge to the stockholders (Rockness & Rockness, 2005). Having describe the types of crimes and the penalties that followed, one can see how each of these examples tie directly to a person or set of people obtaining gain which should rightly be their fellow man's. Thus, these individuals are stealing from their earthly brothers which ties directly to committing evil. Those who will commit evil will do so even more when the stakes are high and financial gain is great.

Propensity for the Success of SOx

From the years of 1913 until the Sarbanes-Oxley (SOx) Act of 2002, there were many laws that tried to provide legislature to govern ethical behavior especially among corporate executives. From 1913 to 2002, there nine major pieces of legislature were passed including SOx (Rockness & Rockness, 2005). Each law had a particular focus. For example, the Owen-Glass Act of 1913 gave rules to govern the operation of banks and their financial reporting. The U.S. Securities and Exchange Act of 1933 prohibited deceit, misrepresentation, and fraud from the sale of company stocks or securities. The FIDCA Improvement Act of 1991 covered fraud and conflicts of interest for executives and officials of companies. SOx covered financial reporting, the requirement for independent auditing, and added many sub-parts that allowed for more severe punishment of executive and officials who committed business misconduct.

The SOx Act of 2002 actually culminated all the known loop-holes in previous laws and worked hard to provide internal controls, independent auditing, certification of documents, and more severe punishments (Romano, 2005). SOx has the propensity for success. SOx also worked to stop executive loans (Romano, 2005). Thus, many of the known issues in laws past were attempted to be corrected with the passing and implementation SOx. The SOx Act of 2002 is by no means perfect but it did provide more legislation to help thwart unethical business practices. In fact, it was so powerful and game-changing that the stock market even took a very large dip in July of 2002 when SOx was passed (Romano, 2005). This was said by multiple people in the legislative body to be evidence that unethical business practices and wrong-doing were being committed. There have been multiple weaknesses identified since the passing of SOx. Ge and McVay (2005) noted that the weaknesses include: accruals of accounts receiving, accruals of accounts payable, inventory, income tax, and expense reporting. So, there are still things that need improvement with SOx and that will hopefully be corrected in the future but it is the best and most successful piece of legislation we have currently.

Known Weaknesses of Sarbanes-Oxley

Ge and McVay (2005) investigated the material weaknesses of the internal controls outlined by SOx. They noted that the key areas of SOx where weaknesses existed were in the areas of training policies, period end and accounting policies, revenue recognition policies, inventory and accrual policies (both accounts receivable and accounts payable), account reconciliation, and policies involving the segregation of duties (Ge and McVay, 2005, pp. 144-149). A training policy, for example, might require the accountants in the company to follow a process outlined in a policy. So, the company needs to train their employees about the policy so that the accountant will know to follow the process outlined. Reynolds (2012) notes an additional area of policy that is affected by SOx. This is the area of establishing a policy and a set of test for outsourcing SOx. In other words a definition would be if a company wants to outsource their SOx compliance, they

must first use the Statement of Auditing Standards (SAS) No. 70 which is an internationally recognized standard developed by the American Institute of Certified Public Accountants (AICPA) (Reynolds, 2012, pp. 402-403). A successful SAS No. 70 audit report demonstrates that the outsourcing firm has effective internal controls as per the SOx Act of 2002. Thus, the policies that are affected in companies should try to counteract these weaknesses and should include new policies to be written by the company to affect the change required for overall SOx compliance. These SOx weaknesses have the ability to affect many reports in the company involving financials, inventory, income tax, expenses, restructuring, and accruals. Therefore establishing these policies is very important.

VIII. FUTURE OF SARBANES-OXLEY AND POTENTIAL REPLACEMENTS

The SOx act was initially put into legislation to repair some of the known holes in the system pertaining to the management and operation of publically traded companies. For years there has been example after example of the leadership of publically traded companies conducting unethical business transactions which left the stock-holder holding the bag and taking the financial loss. Since its enactment, SOx has performed best as a deterrent but does have areas where improvements can be made. Many authors have expressed their criticisms while others have given counterarguments. This article attempts to discuss SOx, known issues, negative effects, opportunity costs, counterarguments, and then give final assessment of the state of SOx along with comments about the future of SOx.

General Requirements of SOx

Drawbaugh and Aubin (2012) point out that the major parts of SOx did the following: established a Public Company Accounting Oversight Board (PCAOB), implemented internal controls, required corporate executives to certify financial document accuracy, and increased the penalties for financial fraud. Brown (2006) adds that the chief executive officer (CEO) and the chief financial officer (CFO) actually are the ones who have to certify the accuracy of the financial documents. Further, Brown (2006) points out that SOx actually requires annual disclosure of internal controls in the form of a report. These are the major overall requirements of SOx.

Known Issues with SOx

Drawbaugh and Aubin (2012) discuss eight issues that are very commonly discussed as they pertain to SOx. These are:

1. Companies are commonly insulating chief-level executives from SOx
2. Prosecutors tend to only pursue common and more typical-type fraud cases
3. Companies use small auditing firms who were exempt from inspections prior to 2010
4. Since the client pays for auditing services, the client often dictates what gets done
5. SOx has not brought increased competition as was planned and only four big auditing firms now exist
6. SOx was not designed to ensure that corporate accountants should know all and be everywhere in the company. So not everything is known
7. SOx has been weakened by the JOBS Act signed by President Obama in April of 2012. The weakening comes from not requiring small start-up companies to comply with SOx
8. There are limits on the auditing companies but not limits on the tax accountants

Brown (2006) adds the following issues:

1. SOx tends to generate an increased cost due to the auditing and internal controls. The cost does not outweigh the benefits
2. The greater independence of accountants can be harmful to companies
3. The prohibition of loans to executives is a public policy error since it basically is telling companies what they can do with their own money
4. Separating accountants and auditing consulting firms can negatively affect audit quality

Negative Effects of SOx

Bargeron, Lehn, and Zutter (2010) point out that SOx has caused negative effects in the form of companies and corporations taking risks. Bargeron, Lehn, and Zutter (2010) conducted an empirical study of United States firms and compared them to companies in the United Kingdom. The data for the study consisted of information collected from 1990 to 2006. The study showed that U.S. firms have reduced their research and development budgets as well as capital expenditures compared to U.K. companies. U.S. companies were found to have increased their cash holdings, as well. Furthermore, initial public offerings in the U.S have declined from 1990 to 2006. All of this has happened since SOx was enacted. This, Bargeron, Lehn, and Zutter (2010) says, is an indication that SOx has negatively affected U.S. firms. The premise is that the less risk U.S. companies are willing to take, the less potential for reward for the companies and the stockholders. Thus, they portray SOx to be harmful.

Opportunity Costs of SOx

Butler and Ribstein (2006) actually go as far as to suggest that there are opportunity costs due to SOx. One such opportunity cost that they note is that SOx makes managerial talent not want to work at U.S. publically traded companies. This, Butler and Ribstein (2006) suggest, is due to increased scrutiny of these individuals, no chance of executive loans, and prohibitions on pay. They also suggest that entrepreneurial companies have now been turned into hall monitors for SOx. Butler and Ribstein (2006) note that this is due to compliance costs, social costs, reduction in the flow of resources, and riskier companies not being funded. They note that the trend has now become to stay private and not become a publically traded company. Butler and Ribstein (2006) conclude by saying that SOx is not worth the opportunity costs that have happened since the legislation was enacted.

Recommended Changes for SOx

Brown (2006) notes that there has been talk to have the states take over the role of SOx. To add to this, Butler and Ribstein (2006) recommend that SOx be amended to:

- Prohibit private lawsuits
- Exempt dual listed securities of foreign corporations
- Exempt all but the largest corporations
- Allow shareholders to opt-out through proxy
- Remove criminal sanctions

All of these seem like reasonable changes when you view the world through the opportunity costs that Butler and Ribstein (2006) presented. But, there is always more than one side to any story. Thus, there are counterarguments that can also be considered for some of the issues and opportunity costs. These counterarguments can affect recommended changes. For instance, Butler and Ribstein (2006) state that SOx is not worth the additional costs but Brown (2006) points out that the estimates of cost over the years have been very weak because the estimates were not based upon real data. Another example presented by Bargeron, Lehn, and Zutter (2010) is that the reduction in willingness by U.S. companies to endeavor in more risky undertakings such as research and development of new technologies has hurt companies and stockholders. On the other hand, less risk is more conservative and could actually yield better stock performance over the long term. To the contrary, this could benefit stock holders. The argument that states should take over the role of SOx has some counterarguments as well. First, this presents a problem in deciding which branch of the state government would be most effective in taking over SOx. Second, the issue of keeping self-interests out of the picture would be very hard. This would show up in the determining of who would benefit most in the state. SOx is indeed a balancing act.

Overall Assessment

Drawbaugh and Aubin (2012) assert the opinion that SOx has been working since 2002. They note that a handful of criminal charges for false statement in financial document certification have been made. Also, there have been 200 Securities and Exchange Commission (SEC) civil cases since 2002. Finally, Drawbaugh and Aubin (2012) point out that SOx has been a sharp deterrent and has created a mindset that accounting firms must produce accurate and true financial reports. Thus, in the view of Drawbaugh and Aubin (2012), SOx has been successful. Holmstrom and Kaplan (2003) note that the governance of U.S. corporations has not been as bad in actuality as has been depicted. They state that executive pay has also actually increased by a factor of 6 over the last two decades. Thus, this also provides some proof that SOx is working and is not totally affecting the U.S. in negative ways.

Major Changes Needed for Future

So what then does need to be done in regards to SOx and how can it be improved? First and foremost, Drawbaugh and Aubin (2012) bring up the point that it must be enforced and this is indeed true. If SOx is not enforced, not many organizations will comply with it. Second, Holmstrom and Kaplan (2003) make the point that NYSE and NASDAQ regulations will affect the PCAOB and these new regulations must be watched closely. Two such examples include: 1) more aggressive monitoring of top management and 2) changes to executive compensation by restricting top executives from exercising options, selling, or hedging stock sales. The JOBS Act of 2012 is also a major concern for SOx that will require changes. Since start-up companies are now exempt from SOx, new regulation may be required to add additional monitoring and penalties to start-up companies. If this is not done, the trend may become that companies become new start-ups instead of building upon existing companies. Finally, and probably the most important thing that needs to be improved with SOx is the trend for companies to stay private to avoid SOx (Brown, 2006). This can be a very bad trend for stockholders since they will not have the opportunity to invest in what could be very profitable endeavors. In fact, this shortens the list of companies that investors can choose from. As the trend to stay private continues, the market becomes more unregulated. Thus, this issue is the most significant thing affecting the future of SOx and is the area where improvements must be made to reverse this trend of privatization.

IX. CONCLUSIONS

It is a common opinion that government should work to protect citizens by passing legislature that protects stockholders from great and substantive monetary losses due to the unethical behavior of corporate executives and officers. Thus, SOx is needed. This does not necessarily protect the citizens from losses incurred due to the management team performing in a manner that is not profitable. Loss can still occur due to poor management. But, what should be legislated to protect stockholders against the unethical conduct of managers, executives, employees, or officers of a publically traded company where stockholders (citizens) can be severely harmed. This harm could be so great that it actually harms the nation and stops the money flow which can shut down the economy. Thus, it is to the government's interest to protect the citizens from severe financial harm due to unethical business practices of corporate executives. The penalties for violating these laws and regulations should be severe to deter potential violators from committing unethical business practices.

Mankind has historically done many unethical and even evil things to steal from their brother in order to gain a buck or two. Noting this, over time mankind has implemented many acts, laws, and regulations to help thwart those that would commit evil by performing business misconduct from doing so. The weaknesses in these laws have left opportunity for those who would commit unethical business practices. But, each subsequent law or act tried to fill in the known gaps from previous laws. We now have the SOx Act of 2002. SOx does a great job of filling known gaps but still has some known weaknesses. SOx has proven to be a great deterrent. Every university with an IT program worth its salt teaches SOx and almost any corporate executive at any major publicly traded company knows about SOx, so it is very effective as a deterrent. These laws (including SOx) play a very important role in protecting the citizens of this country from great financial ruin due to the misconduct of business executives. Therefore, these laws are a necessity and government should continue to stay involved in business as well as continue to improve the legislation to further protect citizens. For all the reasons presented in this article, although not perfect, SOx is viable and needed.

REFERENCES

[1] Addison-Hewitt Associates (2006). *A guide to the Sarbanes-Oxley Act*. Retrieved from http://www. soxlaw.com/ index. htm

[2] Bible, Holy (2000). *King James Version*. Texas: National Publishing Company.

[3] Bargeron, L., Lehn, K., & Zutter, C. (2010). Sarbanes-Oxley and corporate risk-taking. *Journal of Accounting and Economics, 49(1)*, 34-52.

[4] Brown, J. (2006). Criticizing the Critics: Sarbanes Oxley and Quack Corporate Governance. *Marquette Law Review, 90*, 309-335.

[5] Brown, W., Moore, G., & Tegan, W. (2006). *SOA governance-IBM's approach* [Whitepaper]. Rational Software. Retrieved from ftp://ftp.software.ibm.com/software/soa/pdf/SOA_Gov_Process_Overview.pdf

[6] Butler, H., & Ribstein, L. (2006). *The Sarbanes-Oxley Debacle: how to Fix it and what We've Learned*. AEI Press.

[7] Cognizant (2013). Maximizing business value through effective IT governance. *Cognizant 20-20 Insights, (5)*. Retrieved from http://www.cognizant.com/InsightsWhitepapers/Maximizing-Business-Value-Through-Effective-IT-Governance.pdf

[8] Dietz, G., & Gillespie, N. (2012). *The recovery of trust: Case studies of organizational failures and trust repair* [Occasional Paper 5]. London, England: Institute of Business Ethics.

[9] Drawbaugh, K. & Aubin, D. (2012). Analysis: A decade on, is Sarbanes-Oxley working? *Reuters*. Retrieved from http://www.reuters.com/article/2012/07/29/us-financial-sarbox-idUSBRE86Q1BY20120729

[10] Evans, J. (2014). *Quality and performance excellence: Management, organization, and strategy (7th ed.)*. Mason, OH: South-Western, Cengage Learning.

[11] GAO (2009). *Federal Information Systems Controls Audit Manual (FISCAM)*. Retrieved from http://www.gao.gov/new.items/d09232g.pdf

[12] Ge, W., & McVay, S. (2005). The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. *Accounting Horizons*, 19(3), 137-158.

[13] Haes, S. & Grembergen, W. (2009). Moving from IT governance to enterprise governance of IT. *ISACA Journal, 3*, 21-21.

[14] HBR (2013). *HBR's 10 Must Reads on Strategy*. Boston, Massachusetts: Harvard Business Press.

[15] Herman, D., Scalzi, G., & Kropf, R. (2011). IT governance best practices. *Aspen Advisors*. Retrieved from http://www.aspenadvisors.net/results/whitepaper/it-governance-best-practices

[16] Holmstrom, B., & Kaplan, S. (2003). The state of US corporate governance: what's right and what's wrong?. *Journal of Applied Corporate Finance*, 15(3), 8-20.

[17] Johnson, A., & Toth, P. (2007). *Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems.* Retrieved from http://csrc.nist.gov/publications/drafts/nistir-7328/NISTIR_7328-ipdraft.pdf

[18] Lajili, K. (2012). Towards building a human-capital based governance framework. *Journal of Management Policy and Practice, 13(3)*, 13-30.

[19] LRN (2006). *The impact of codes of conduct on corporate culture: Measuring the immeasurable* [Whitepaper]. Retrieved from http://www.ethics.org/files/u5/LRNImpactofCodesofConduct.pdf

[20] Lunardi, G., Becker, J., & Macada, A. (2009). The financial impact of IT governance mechanisms' adoption: An empirical analysis with Brazilian firms. *Proceedings of the 42nd Hawaii International Conference on Systems Sciences (HICSS'09)*, 1-10.

[21] Maizlish, B. & Handler, R. (2005). *IT portfolio management step-by-step: Unlocking the business value of technology*. Hoboken, New Jersey: John C. Wiley & Sons.

[22] Milne, K. & Bowles, A. (2009). *How IT governance drives improved performance* [Whitepaper]. IT Process Institute. Retrieved from http://www.isaca.org/Groups/Professional-English/governance-of-enterprise-it/GroupDocuments/ITPI_IT_Governance_summary_paper.pdf

[23] MN IT Services (2012). *State of Minnesota IT governance framework* [Whitepaper]. Retrieved from http://mn.gov/oet/images/06012012_IT_Governance_Framework.pdf

[24] Moeller, R. (2013*). Executives guide to IT governance: Improving systems processes with service management, COBIT, and ITIL*. Hoboken, NJ: John Wiley & Sons.

[25] National Computing Centre (2005). *IT governance: Developing a successfully governance strategy* [Whitepaper]. Retrieved from http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam-OLD/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf

[26] NIST (2010). *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*. Retrieved from https://www.fismacenter.com/SP800-53A-final-sz.pdf

[27] NIST (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-53r4

[28] Pirani, J. & Salaway, G. (2008). Queensland University of Technology: Three generations of IT governance (and counting). *EDUCAUSE Center for Applied Research*.

[29] Rajan, R., & Zingales, L. (1998*). The governance of the new enterprise* (Working Paper). Retrieved from http://www.nber.org/papers/w7958.pdf

[30] Reynolds, G. (2012). *Ethics in information technology (4th ed.).* Boston, MA: Course Technology, Cengage Learning.

[31] Rockness, H., & Rockness, J. (2005). Legislated ethics: From Enron to Sarbanes-Oxley, the impact on corporate America. *Journal of Business Ethics, 57*, 31-54.

[32] Romano, R. (2005). The Sarbanes-Oxley Act and the Making of Quack Corporate Governance. Faculty Scholarship Series, Paper 1919. Retrieved from http://digitalcommons.law.yale.edu/fss_papers/1919

[33] Sharma, D., Stone, M., & Ekinci, Y. (2009). IT governance and project management: A qualitative study. *Database Marketing & Customer Strategy Management, 16 (1)*, 29-50.

[34] Spicer, D. & Pirani, J. (2008). Reforming IT governance at Berkeley: Introducing an enterprise perspective to a decentralized organization. *EDUCAUSE Center for Applied Research*.

[35] United States (2002). *United States Public Law 107-204*. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf

[36] Wilson, W. (n.d.). *Conceptual model for enterprise governance* (Presentation). Retrieved from http://sunset.usc.edu/GSAW/gsaw2009/s5/wilson.pdf

Author's Biography

Charles Madewell is an expert in information architectures, data science, and simulation. He holds a Bachelor of Science and Master of Science in engineering from the University of Alabama in Huntsville. Mr. Madewell is scheduled to be conferred with the Doctor of Computer Science in June 2015 from Colorado Technical University in Colorado Springs, Colorado.