

## **Information Trust and Compliance issues**

*Exploring the potential for an unified compliance policy approach for publicly listed companies in Health care industry complying with both Sarbanes Oxley & Health Insurance Portability & Accountability Act*

**Sidhartha Bhandari**

**MS – Technology Management**

**Trustworthy Computing**

**Information Security and Management**

**May 4<sup>th</sup>, 2006**

## **Index**

<b>Overview.....</b>	<b>2</b>
<b>Review.....</b>	<b>3</b>
- Sarbanes Oxley Act, 2002 (SOX)	
- Health Insurance Portability and Accountability Act, 1996 (HIPAA)	
<b>Guest Speaker Summary.....</b>	<b>5</b>
<b>Identifying the overlapping unification objective of SOX and HIPAA.....</b>	<b>7</b>
<b>Emerging trends in developing unified compliance best practices.....</b>	<b>9</b>
<b>Cost and Benefits of compliance unification.....</b>	<b>10</b>
<b>Conclusion.....</b>	<b>12</b>
<b>Appendix.....</b>	<b>13</b>
<b>References.....</b>	<b>15</b>

## **Overview**

With information management coming forefront in many managerial decisions, it is becoming an important priority for companies across all verticals to understand and comply with various regulatory requirements.

In United States, given the growing concern about accountability and security of consumer's personal information organizations are legally required to comply with regulatory requirements such as Health Insurance Portability & Accountability Act. At the same time many of these large organizations have also listed themselves in the stock market. In order to be listed in the stock market Securities Exchange Commission requires that these companies must comply with the Sarbanes Oxley Act. This is done to safe guard the investor interests and prevent accounting frauds like Enron & World-com from happening.

Faulting on either one of these regulations can quickly result into huge loses both monetary and prestige for the corporation. Individuals (CEOs, CFOs) if found guilty can also face criminal proceedings due to corporate negligence. Consumers may be under threat too because of information loss that can result in identity thefts & personal damages. Through discussions with various in-class guest lecturers and research it is evident that regulatory compliances like SOX and HIPAA describe what needs to be done but they do not go into the details of how it is to be done. This therefore leaves room for interpretation which result in significant costs implications. The External auditors, understandably in such situations, have to take a more conservative look at these organizations while evaluating them. For the organization all this means higher cost of doing business and increase in associated risks.

Companies have to invest time and resources in taking precautions to manage risks in a pool of compliances. The push to have the safest route for the organization under such situations lands up making the organization over complied than under thereby adding to the costs.

In the light of the above explained situation this report aims at understanding Sarbanes Oxley and Health Insurance Portability and Accountability. We look at various areas of the compliances which organizations should consider while preparing their regulatory compliance policy. A thorough analysis can provide better idea of the amount of resources required. This works best in the interest of the organization that is planning to optimize the amount of resource required for compliance. Moving forward we explore some of these areas to develop an understanding of costs and benefit of unified compliance.

### **Reviewing Sarbanes Oxley Act and HIPAA**

Sarbanes Oxley - Act of Congress – was formed in 2002 following large corporate financial reporting frauds; incorrect accounting practices including the involvement of accounting firms like Arthur Anderson which rocked the investor confidence in the market place. Taking a stern step in response to such activities SOX was create to improve corporate governance by making the management of the respective organization liable for any attempt to hide or incorrectly present the performance of the organization.

The Act, which consists of 11 chapters, states the responsibilities of the corporation and the role of accounting firms.<sup>1</sup>

#### *Chapter 1*

SOX first took the task of setting up Public Company Accounting Oversight Board (PCAOB) with powers to adopt or modify auditing practices, control quality, maintain ethics and independence standards for public companies. PCAOB's actions are subject to review by SEC. PCAOB is responsible to check controls regularly in audit firms and investigate violation of audit practices by audit firms.

#### *Chapter 2*

SOX cracks down on auditor independence by defining services an auditor can or cannot perform. As describe in the class Arthur Anderson's steady source of revenue coming from consulting services hindered its neutrality to play the fair role of the Auditor.

Therefore SOX has now defined prohibited consulting services for audit firms. Audit partner rotations and regular reporting of the audit committee are now required to maintain top level of external auditor independence.

*Chapter 3:* Section 302, most common of all, looks particularly at the Management's (i.e. the CEO & CFO) responsibility to certify the correctness of the organizations financial statement. This chapter emphasizes the need for an audit committee and details the various penalties & punishments.

#### *Chapter 4 - Enhanced Financial Disclosures*

Two of the most widely mentioned compliances are Sox 404 & 409 in this chapter.

SOX- 404 looks at requirements for annually reporting the controls in place in an organization, their effectiveness and significant deficiencies. It is also identified as the responsibility of the External Auditor to test these and attest the company's fair state of internal controls. A snap shot of this statement from a publicly listed company is mentioned on Exhibit 1. SOX 409 states that the real time reporting of changes in the functioning of an organization that may affect the financial performance. This is to mitigate the hindrance in transparency of the financial health which earlier was limited due to the reporting taking place only once a year.

#### *Chapter 5*

A major influencer in the investors' decision has been the role of securities analyst. This chapter addresses the analyst conflicts of interest.

*Chapter 6 & 7:* These look at commission's resources and authority. These include additional reports by the SEC.

#### *Chapter 8 – 11*

Consist of Corporate and Criminal Accountability, White – Collar Crime Penalty Enhancements, Signing of Corporate Tax Returns, addressing corporate fraud and accountability. These sections explain the penalties for failure to comply with the

regulations. Chapter 8, for instance mentions that company's financial and audit records cannot be destroyed or fabricated. Auditors are required to manage the audit work following the end of financial year for five years.

## **HIPAA**

Health Insurance Portability and Accountability Act of 1996 contains the rules to improve medical security and privacy. The procedures identified here are with the aim to simplify administration of health care billing.

The standards addressed in the following areas are<sup>2</sup>:

*Insurance Portability* – Based on this health care providers are required to maintain continuity of service as individuals move from one policy to the other.

*Fraud Enforcement* – This increases Federal government's authority to combat Medicare and Medicaid frauds.

*Administrative Simplification* – Given the requirement for flow of information through various medical entities HIPAA looks into improving efficiency and effectiveness of health systems while protecting the confidentiality of electronic health information.

HIPAA regulation requires Healthcare organizations to develop and enforce personal health information disclosure policies and procedures. Patients have to the right to access and amend their own information. HIPAA advocates setting up fair information practices to provide people the visibility into the way their information is being used. As healthcare information needs to flow through various entities like hospitals, insurance agencies and pharmacists HIPAA requires organizations to maintain audit trails of health information disclosures.

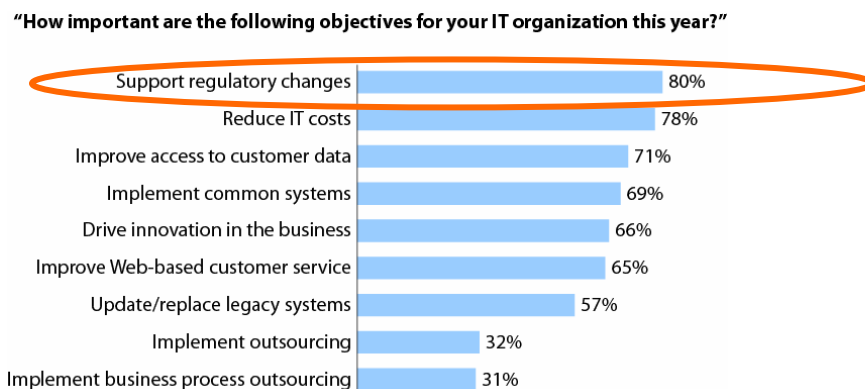
## **Guest Speaker Summary**

The purpose of reviewing these regulatory Acts has been motivated by various discussions in the class. Initial discussions/ presentation - especially on "Information

Trust and Compliance Issues”- by Deron Grzetich from Protiviti focused on details about Sarbanes Oxley. It was interesting to receive an External audit organization’s perspective on the compliance. This presentation in class was deeply motivating to understand the ambiguity associated with implementing compliances. Through further interactions with the speakers it was also interesting to learn that organizations also need to comply with many other regulations including HIPAA and GLB at the same time. Some statistics presented on three questions from the “CFO-IT Magazine interview of 153 CFO/CEO’s” during the presentation highlighted the need for simplifying and developing unified compliance adoption approaches to counter ambiguity.

According to the numbers presented 94% of CEO’s interviewed admitted that during SOX Section 404 audit, many failures and deficiencies could be attributed to IT. 74% of CEO’s felt regulators were not clear in communicating the details of what makes adequate IT controls. On questioning them about the IT auditor’s level of understanding regarding the IT components of the internal control to audit section 404 , 71% fell in the category of answering ‘No’ or ‘Unsure’.

This project report, through interactions and research, is an attempt to now address the situation of multi-compliance environment presented in class from a CEO or management’s perspective.



Base: 150 decision-makers at North American insurance carriers with annual revenue above \$500M who answered “very important” or “critical” (multiple responses accepted)

*Source: Forrester, June 2005, Trends “Drivers And Trends For IT In Insurance”*

A Forrester report also highlights the importance healthcare providers in the US are placing on regulatory changes. It is the top most priority for about 80% of IT organizations within the Insurance companies which reinstate the importance.

Given such uncertainties how can CEOs comply with regulations while keeping costs to the minimum? Are there overlaps in complying with different regulations which can be beneficial? If so, can identifying these gaps reduce costs while preparing an organization for compliance?

These are some of the questions management teams should consider as part of framing a compliance adoption policy.

### **Identifying the overlapping unification objectives of SOX and HIPAA**

SOX & HIPAA as mentioned above are driven by different needs and circumstances. According to IDC, despite of complex nature of compliances, there are common parts which can be found in the underlying base framework. Common controls once identified can be incorporated in the organization's compliance and security policy and can be assessed for effectiveness.

Some of these areas of unification based on research are as follows:

#### *Maintaining Information Security*

The regulations lay emphasis on securing information. Setting up levels of access to avoid data modification and provide transparent ability to view any changes made are key requirements. Organisation must demonstrate their network's ability to prevent data corruption or asses their vulnerability to intrusion that may result in stolen or altered data. Importance is laid on real – time monitoring of data. Regulations require regular assessments for technical vulnerabilities in network devices, servers and applications. In financial services industry, for instance, Visa and MasterCard are making use of the Vulnerability Detections services to quarterly scan services required for merchants and service providers<sup>3</sup>. Various operating systems are required to have multi-level security to store local data in the organization. In most cases disaster recovery planning is also

coming into play that is requiring organizations to keep back up all the relevant data regularly<sup>4</sup>.

#### *Email & communication security*

Information technology has made email a common medium for flow of information in the functioning of a business. With this there also is the opportunity for risk. The compliances look at controlling, monitoring and restricting the use of email appropriately. They advocate setting up role based access controls to ensure that the information is not left to all the people in the open. As the number of emails is increasing so are the spam mails. Compliances enforce that distinct processes be in place to separate compliance related material from the junk mail. Losing required information can have significant consequences on the business.

#### *Evidence of controls*

Documentation and maintenance of documents is a key compliance. The regulations require public companies to establish, document and assess the effectiveness of their internal controls. HIPAA requires organization to prove that their data has not had any unauthorized alteration and is trust worthy. The details of the process use must be documented and made available explicitly. Taking reference from Andy Retrum's (from Protiviti) presentation on "Vulnerability Management & External Penetration" discussing about the importance of risk & control - in SOX the organizations must now explicitly explain its controls & their present state which needs to be documented. This is one of the reasons why now financial statements of publicly listed companies have a mention about the COSO framework examined by the auditor as a measure of company's risk compliance. Capturing compliance related documents is important to demonstrate the proof of control.

#### *Data Storage reliability*

The regulations have propelled the boom for data storage industry. Terms like Enterprise Record management and content management have become important with organizations which are thinking about making there IT systems robust. Companies working to comply

are now thinking of best practices to help them manage their records and also update/keep the repository of information up to date.

*Audit trail management*

As described in the explanation for regulations earlier, it is important to maintain audit trail of the information being shared across all levels internally and externally. This could be financial information or Health information. Log monitoring is required to help ensure compliance<sup>3</sup>.

IT Compliance Institute: The Global Authority for IT Compliance Information and Alerts				
Technology Impact Area	CobiT Control Objectives	COSO ERM Framework	HIPAA § 164	Sarbanes Oxley
Leadership and High-Level Objectives	X	X	X	X
Audit and Risk Management	X	X	X	X
Systems Continuity	X	X	X	
Records Management	X		X	X
Design and Implementation	X		X	X
Systems Acquisition	X	X	X	X
Operational Management	X	X	X	X
IT Staff Management and Outsourcing	X	X	X	
Technical Security	X		X	X
Physical Security	X		X	
Monitoring, Measurement, and Reporting	X	X	X	X

Source: "IT Compliance Institute." IT Compliance impact matrix. IT Compliance Institute. <<http://www.itcinstitute.com/ucp>>.

Table mentioned above is useful in highlights more commonalities in the HIPAA and SOX framework. For instance, Audit and Risk Management needs to be performed across all regulations to ensure that the management is continuously monitoring its systems and is in control of the process. Repeating this multiple times for the same organization may not make as much sense as it would to include this impact area as part of the unified compliance practice policy for the company. In various other practical applications CoBIT (Control objective for IT) also finds its use in harmonizing with frameworks like COSO, IS1799 and ITIL.

**Emerging trends in developing unified compliance best practices**

- Life science companies, having to comply with HIPAA, SOX and other regulations are considering the options of creating cross functional teams to work across multiple regulation compliances. Sixty-two percent of such public

companies are using cross-functional teams for SOX compliance; and in 72 percent of that group, the finance department is assuming responsibility for the leadership position<sup>5</sup>.

- Across industries Corporations are beginning to realize the need for concepts such as Enterprise Records Management and Enterprise Content management. Organizations for effective compliance. They are beginning to understand the significance of information management and are making efforts to properly identify, store, edit and manage throughout the information lifecycle as an asset of the business. For instance organizations complying with both SOX and HIPAA are preparing policies for prioritizing data types for retention and are looking for optimal cost storage device types to save data based in its importance.
- Technology companies are seizing this opportunity to develop platforms due to the growing need in the market place for multiple compliances. Leading players include Oracle, IBM, VeriSign EMC, Humming Bird and Symantec.(Refer to Exhibit 2 for list of vendors and compliance services)
- IT Compliance Institute and many others are focusing on developing Unified Compliance Projects and are working on IT to bring compliances together.
- Leading audit practices have also made attempts to harmonize COBIT with SOX and Gramm-Leach Bliley Act which demonstrates the potential of compliance unification as a key differentiator in the market place.

### **Costs and Benefits associated with compliance unification**

Reduction in regulatory compliance costs has been a major driver for the growing popularity of setting up common compliance practice. In a recent citation made by IT compliance Institute, a May 2004 report by Gartner, Inc., estimates that public companies adopting compliance management architecture will spend up to 50 percent less on compliance by 2006 than companies without one.

### Costs of developing a common compliance framework

- In order to create a unified company practice for regulation, investments are required in developing a common matrix and procuring technology to support unified compliance initiatives.
- Moving to common compliance technologies may have hidden costs associated with training and maintenance
- Cost of documenting and upkeep of common objectives
- The risk of legal liability may arise if the common compliance model misses out on addressing all the required issues.

### Benefits

- Developing a unified compliance practice can help an organization reduce complexity and workload for various departments which are part of the compliance project.
- Alignment of requirements is beneficial in standardizing regulatory issues into a common matrix.
- In case of any changes or modifications to the regulatory rules, organizations can easily adapt its practice by referring to its unified compliance policy thereby making it easier to track changes in the ever growing regulations arena.
- Unifications enhances effective use of knowledge among various compliance requirements
- Combining compliance regulations to one platform can provide better and easier management control<sup>6</sup>
- A common technology platform can be mapped to reduction in infrastructure requirements required to achieve compliance. These can result in hardware, software and other resource savings.
- Given a common platform, it may also be helpful for companies to reduce the time to audit. This may translate into more valuable use of an auditors' time in evaluating the company.

## **Conclusions**

Publicly listed corporations in the health care industry complying with SOX and HIPAA must take the initiative to drive a model of compliance in the organization keeping in mind that there are avenues of unification which can drive costs down while ensuring the maximum value & full compliance. External Auditors play a critical role in auditing and certifying the compliance framework of a corporation but it is the responsibility of the Corporation's leadership to have their own framework in place in order to reduce the expenses on regulatory compliance.

The unification approach allows bringing together common parts of a multitude of compliances. Both external auditors and Corporations can work closely to ensure full compliance at lower costs.

Efforts to develop Unified Compliance models have been individual to ones own industry so far. But as the regulatory compliances evolve its application is being valued much more than before. Large scale benefits may exist in understanding and creating models across industries that cater to a multitude of compliances on a single platform.

A key take away from the lectures, class discussions, research and from the overall course has been that regulatory compliance are here to stay and become part of doing business. It must be viewed as an opportunity is disguise rather than a painful one time task. How well corporations manage adapting to it is dependent on its culture, resources and policies.

# Appendix

## Exhibit 1

### ■ Report of Independent Registered Public Accounting Firm

#### Board of Directors and Shareholders Eli Lilly and Company

We have audited management's assessment, included in the accompanying Management's Report on Internal Control Over Financial Reporting, that Eli Lilly and Company and subsidiaries maintained effective internal control over financial reporting as of December 31, 2005, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (the COSO criteria). Eli Lilly and Company and subsidiaries' management is responsible for maintaining effective internal control over financial reporting and for its assessment of the effectiveness of internal control over financial reporting. Our responsibility is to express an opinion on management's assessment and an opinion on the effectiveness of the company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, evaluating management's assessment, testing and evaluating the design and operating effectiveness of internal control, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, management's assessment that Eli Lilly and Company and subsidiaries maintained effective internal control over financial reporting as of December 31, 2005, is fairly stated, in all material respects, based on the COSO criteria. Also, in our opinion, Eli Lilly and Company and subsidiaries maintained, in all material respects, effective internal control over financial reporting as of December 31, 2005, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the 2005 consolidated financial statements of Eli Lilly and Company and subsidiaries and our report dated February 13, 2006 expressed an unqualified opinion thereon.

*Ernst + Young LLP*

Indianapolis, Indiana  
February 13, 2006

FINANCIALS

## Exhibit 2

Interwoven	Interwoven Records Manager	<ul style="list-style-type: none"> <li>● Manages physical and electronic records with a single policy manager</li> <li>● Allows for declaration of a project, workspace, folder, or file for application of policies</li> <li>● Allows for record declarations based on metadata to enable policies to be applied consistently and based on company policy, not user opinion.</li> </ul>
OpenText	Livelink Records Server	<ul style="list-style-type: none"> <li>● Meets DoD 5015.2 requirements</li> <li>● Allows for application of classification of metadata to submitted documents to enhance searches</li> <li>● Invokes retention and disposition rules upon classification of a record</li> <li>● Implements Microsoft COM architecture to provide access to business functions</li> <li>● Allows admins to periodically review vital records to ensure appropriate classification and disposition</li> </ul>
Stellent	Stellent Records Management	<ul style="list-style-type: none"> <li>● Controls access at any level of granularity</li> <li>● Uses browser-based interface to create and administer file plans</li> <li>● Able to classify any piece of content as a record</li> <li>● Defines records using defined criteria</li> <li>● Includes email and attachments</li> <li>● Automates the workflow process while maintaining the level of manual review</li> <li>● Searches, views, and prints, audit trail info from the Web browser</li> <li>● Generates reports on retention schedules and file plans</li> </ul>
EMC	Documentum: Records Manager	<ul style="list-style-type: none"> <li>● Certified as compliant with DoD 5015.2</li> <li>● Helps achieve compliance with SOX, HIPAA, and 21 CFR 11</li> <li>● Provides multiple user interfaces as desired</li> <li>● Auto-classified records in the EMC Documentum repository, reducing manual operations and improving productivity</li> <li>● Tracks retention schedules and applies record-keeping rules uniformly and automatically</li> <li>● Controls and audits access to records throughout their lifecycles.</li> </ul>
Hummingbird	Hummingbird Enterprise	<ul style="list-style-type: none"> <li>● Single shared repository for management of in-process and final records of any physical or electronic media type</li> <li>● Designed to help meet SOX, DoD 5015.2, SEC, NASD, HIPAA, PIPEDA, and FDA requirements</li> </ul>

*Source: Record Management Systems Market Trends, Faulkner Information Services*

## References

1. Weirich, Thomas, W. Rouse Robert. "Sarbanes-Oxley Bill: New Challenges for the Financial Professional." © 2003 Wiley Periodicals, Inc. VL: 14 NO: 2 PG: 55-61, 2003 January/February 2003
2. Volonino, L, Robinson, S. Principles and Practices of Information Security. New Jersey: Pearson Prentice Hall, 2004.
3. "IT Compliance Institute: The Global Authority for IT Compliance Information and Alerts." IT Compliance Institute - Vendor Details. VeriSign. <<http://www.itcinstitute.com/ucp/full.aspx?id=10>>.
4. Newman, Henry. "HIPAA and SOX: What You Need To Know." Enterprise Storage Forum.com May 20, 2005  
<<http://www.enterprisestorageforum.com/continuity/features/article.php/3506751>>.
5. Finical, Vega. "Centralizing Compliance for Competitive Advantage." Common issues addressed by life sciences regulations include control and record accuracy. Jun1, 2005. BioPharmInternational.  
<<http://www.biopharminternational.com/biopharm/article/articleDetail.jsp?id=166177&pageID=1>>.
6. Sukumaran, SreeKumar, Dhulipala Ramesh. "An integrated platform for regulatory compliance in Banking." (2006) 146 - 147. <Source: [www.infosys.com/industries/banking/white-papers/Infosys-Integrated-Platform.pdf](http://www.infosys.com/industries/banking/white-papers/Infosys-Integrated-Platform.pdf)>.

## Additional Reading

- Brenner, Bill. "CSO INTERVIEW: Regulatory pain is a two-way street." June 30 2005 <CSO INTERVIEW: Regulatory pain is a two-way street>
- "Effective Compliance Practices:" December 2004 [www.trustmarquesolutions.com/security/documents/compliance.pdf](http://www.trustmarquesolutions.com/security/documents/compliance.pdf)
- "Effective "The Sarbanes-Oxley Act" (L. Paine), Harvard Business School Case 9-304-079, July 2004.