ETHICS AND COMPLIANCE IN CORPORATE AMERICA: WILL THE SARBANES-OXLEY ACT RESTORE CONFIDENCE IN WALL STREET?

Joseph Valof, Esq.
Richard Menard

About the Authors

Joseph Valof, Esq. is the founder and Principal of OnLine Counsel[sm], Onsite Counsel[sm], and Corporate Compliance Services™ [CCS]. Since 1989, Joe has provided in-house corporate legal services to high-tech companies as a 'vertual' IGC [Independent General Counsel], as well corporate governance support to management. Joe has also authored several business/legal 'white' papers [available at: www.nanosft.com/igc]. CCS acts as a 'Resident Agent' for companies who require a local MA presence and also provides management support to small high-tech companies with its annual shareholder and director meetings, minute book maintenance, etc.

Richard A. Menard is the founder and principal of Cuatro, Inc., a business solutions architect consultancy, which takes a rule-based approach to designing systems and software. Richard has worked with clients in health care, insurance, financial services, high tech, and lifesciences serving as a business analyst, system architect, or technical developer. Richard has authored a number of articles for the IBM Developer Works on business and domain modeling, and has recently been recognized by Telelogic Corporation for his work on regulatory compliance and requirements management.

Introductory Statement by Michael Lissack*

Corporate ethics in the twenty-first century is a misnomer. What we have is a lack of personal ethics being applied by members of society simply because their actions take place in corporate settings. The same people who would not steal from friends and neighbors are happy to help themselves under the guise of "the company." Martha Stewart's plea for a shorter sentence epitomizes the problem, "my company needs me." In such an environment rules and procedures such as Sarbarnes-Oxley serve not only as an enforcement tool, but more importantly as a behavior check. By forcing corporate employees at senior levels to stop and examine their activities (at least for the purpose of signing a report) the formerly inviolate shield of "its the company doing it" is pierced and actions for a moment become personal. I have often wondered if the failure of MBA programs to screen candidates for personal values means that we have spent the past thirty years giving more and more powerful tools to those who were ethically challenged from the start. What kind of a "profession" gives its highest honors to the Andrew Fastows? SOX is a start but what we really need is mandatory Sunday school.

Michael Lissack is the Director of the Institute for the Study of Coherence and Emergence. He endowed the Lissack Chair for Social Responsibility and Personal Ethics at Williams College and serves as a Professor of Management at the Central European University in Budapest. /Worth/ magazine recognized Lissack in 1999 as one of "Wall Street's 25 Smartest Players," and again in 2001 as one of the 100 Americans who have most influenced "how we think about money." Lissack may be best known, however, as the "whistle blower" who exposed numerous illegal and unethical practices of Wall Street firms beginning in 1995. In the years since the US Government has recovered more than $250 million and the investment practices of many state and local governments have been revised as a result of Lissack's initiative.

Preface

The primary goals and aims of this essay are: (1) for the reader who has been harmed by the injustices of some of our corporate leaders, the paper provides an overview and understanding of the remedies available, if any, and how best to pursue them; (2) for the reader responsible for governance and compliance for his company, the paper provides an overview and understanding of the new Sabarnes-Oxley Act, and how best to implement internal controls for compliance; and (3) for the general reader, a feeling of comfort that Wall Street's confidence will be restored.

This paper is organized into two distinct parts [Part I and Part II], both parts, however, are integral and fundamental to conveying the titles complete message. Part I takes the reader through a [brief] historical tour of ethics in America up to the 20th Century. The questions one might ask then are: 'What went wrong in the 21st century' 'How do we correct the situation', 'What remedies, if any, does an injured party have to recover damages suffered as a result of the acts and/or omissions of some of our most powerful corporate leaders' and, most importantly, 'What does the future hold for our future corporate leaders, the workplace, and the American investor. Part II provides the reader with an overview and understanding of the strategies required to comply with the new Sarbanes-Oxley Act [commonly referred to as "SOX" or the "Act"] and focuses on the management perspective of building and sustaining a compliance initiative. The question one might ask is: 'How can I successfully, with minimum cost and resources, seamlessly implement and comply with the Act'. Part II, hopefully, provides the business executive responsible for complying with the Act the knowledge and tools to the implement a systems approach to achieve [complete] transparency from the corporation's normal business activities and routines. The goal of Part II is not to recommend a specific vendor configuration, but to

highlight the significant components which together will help organizations to sustain compliance and outline the major elements of a program that will help to carry out top management policy for running a compliant enterprise. Appendix I provides a specimen of a corporate ‘Ethics Policy’ which meets, in essence, the Acts requirements.

The authors appreciate and thank Michael Lissack for his thoughtful introductory statement.

Introduction

Part I: ETHICS AND COMPLIANCE IN CORPORATE AMERICA

Historical Overview of Ethics

Ethics in the Workplace

Officer and Director Responsibility and Liability

Corporate Governance and Compliance Under Sarbanes-Oxley

Remedies for Redress;Veil Piercing

Part II: Corporate Governance and Regulation

Introduction

The Tone at the Top

Risk Management

Internal Controls

The Need for a Compliance Information Architecture

Components of Compliance Information Architecture

The Bright Side – Benefits of Good Governance

Summary

Appendix I: Business Conduct and Ethics Policy- SPECIMEN

Introduction

"Power tends to corrupt and absolute power corrupts absolutely". British Historian Lord Action, 1887

While the country struggles to contain and eradicate corruption in the American workplace, corporate executives and their accountants are busy developing and scheming to devise new ways and methods to 'cook the books' to impress Wall Street and ultimately their own self-enrichment and gain. As this paper illustrates, the demands placed on corporations over the past several years by management and Wall Street to produce, produce, and to produce even more, has caused managers and their Boards to ignore good common ethical behavior and take whatever means were available to present a set of financials that inflated the company's stock price to impress Wall Street and investors. In fact, management and their Boards authorized and approved [although the evidence in some cases show such approvals to be dubious], unusual perks in the form of outrages salaries, huge outright stock grants [way below market value], stock options, personal loans with no interest and forgiveness provisions, etc. The fact that many company Boards consists of inside directors [with personal self-interests], as opposed to outside directors, was a critical factor in allowing these ongoing abuses to continue. In most instances, the judgments and decisions of inside directors are not totally independent decisions. It is the author's opinion that as a result of all these unusual perks, greed overtook the minds and bodies of our corporate leaders, which ultimately caused their downfall and, of course, bankruptcy of the companies they were hired to grow and protect. As a result of these bankruptcies, many [innocent] people lost their jobs as well as their retirement benefits, pensions, and investments. Additionally, shareholders and investors also lost their investments. Other corporate governance abuses used by our leaders to avoid detection and liability included setting up separate legal entities, both domestically and off-shore with the deliberate intent to deceive investors

and Wall Street. The next question one might ask ‘Does a private citizen who has been harmed by these abuses have a right of action against those executives to recover their losses, and, if so, what are the remedies and how best to pursue them’. As we have seen, the federal Government has vigorously pursued and prosecuted these executives, however, this has not helped the private citizen to get whole. As described in this paper, there are numerous legal remedies available, including an important one, but rarely used, called ‘veil piercing’. Although this remedy is difficult to pursue, it could serve as a powerful litigation weapon if new legislation [either federal or state, or both] were to be enacted to provide more liberal guidelines for its use. Also, it is obvious that the need for more independent board members has become a very critical component in the continuing quest for good corporate stewardship for a public company. Having a more independent Board, would provide the company with the checks and balances required for reducing corruption at all levels of the company.

Companies are always struggling under the weight of managing a host of new and detailed industry regulations. The war on compliance and ethics, however, began with the passage of the Sarbanes-Oxley Act in 2002. Despite its many ambiguities, this Act is probably the most significant piece of legislation affecting business since the Great Depression. The implementation of Sarbanes-Oxley has helped, somewhat, to bring the issues into focus and force company executives into compliance, something they should have been doing all along. The Act has also strengthened and extended the long standing Securities and Exchange Acts of 1933 and 1934 by creating additional reporting demands on corporations whose stocks are traded in US markets. The Act also [greatly] increases the non-compliance penalties for the Board of Directors, CEO, CFO, the Chief Audit Executive and other internal and external audit partners. The Act also applies to many private and international enterprises that leverage capital markets and do business with various governmental agencies, such as [to name a few], the Environmental Protection Agency, Federal Communications Commission, Federal Trade

Commission, and other similarly situation federal agencies. The additional reporting demands are an attempt to rectify the loss of confidence in capital markets in the wake of Enron and other Wall Street scandals. The stakes are high for governments, shareholders, and corporate management. It is a law that cannot be ignored. Yet, the full impact of SOX is still not readily understood by most companies today. Hopefully, this paper will provide the insights to help understand the Act's requirements.

SOX-specific enterprise requirements need to be proactively managed. In addition, many self-imposed enterprise governance work practices associated with SOX such as risk management, IT portfolio management, and internal controls self assessment must also be implemented internally, integrated into day-to-day work discipline and closely managed. This is a new compliance era and the cost-of-compliance must be made a part of the business model so that the company can achieve significant business benefits while absorbing the compliance costs. Last but not least, the Act also mandates that pubic companies adopt a 'business ethics' policy; a typical ethics policy is included in appendix I for information purposes only. Having such a policy could help reduce fines and jail time for corporate criminal offenses.

Because of these needs, companies are looking for strategies and systems that can get this remediation work done quickly. In addition, a need has arisen for a new level of performance monitoring and assessment (i.e. performance management) to ensure that the enterprise stays on track. These same companies are also looking for management systems and automated systems that can sustain compliance and provide management oversight at the same time. The problems associated with managing industry regulations and virtual teams are of paramount concern. They encompass the difficulties associated with the scope and complexity of enterprise-wide collaboration, the many new work disciplines that need to be instituted, and a whole new level of process

management and information management that are required. This paper, hopefully, puts these issues into perspective by defining what is known as a "control architecture".

Part I: ETHICS AND COMPLIANCE IN CORPORATE AMERICA

Historical Overview of Ethics

The origins of ethics and morality and their history, is somewhat elusive, but as best as can be determined by historians, goes back at least to the age of Socrates [c.470-399B.C.], but the exact origins are unknown and impossible to trace. The concepts, however, continue today, into modern times, as further explained and amplified in the next section.

Random House Dictionary of the English Language [1970], defines the terms 'ethics', 'ethical' and 'morality' respectively as follows: "The body of moral principals or values of a particular culture or group'; "Pertaining to or dealing with morals or principals of morality"; Conformity to the rules of right conduct; moral or virtuous conduct". From a legal perspective, Black's Law Dictionary, Revised Fourth Edition [1968] define the terms 'Ethical' and 'Moral Law' respectively as follows: "Professionally right or befitting; conforming to professional standards of conduct"; "the law of conscience; the aggregate of those rules and principals of ethics which relate to right and wrong conduct and prescribe the standards to which the actions of men and women should conform in dealings with each other [announced in Moore v. Strickling, 46 W.VA. 515, 33 S.E. 274, 50 L.R.A. 279]. In their book 'A History of Western Ethics' [Garland Publishing, 1992], Lawrence C. Becker, Editor and Charlotte B. Becker, Associate Editor, the author's take the reader through the various historical movements [by various contributors] from Presocratic Greek through the 20th Century Anglo-American time span. One may ask, what

went wrong in the 21st century that brought the country and the American workplace to the position it now finds itself struggling to reform. Have our schools and colleges [and our educators] failed us, have we lost our ethical upbringing that our forefathers instilled in us in the pursuit of corporate and/or individual gain; has the corporate 'bottom line' objective overtaken our corporate leaders to the point of committing fraud and deceit in the workplace.

Ethics in the Workplace

The term 'business ethics', as used in and referred to, in the workplace, was first coined around the 1970s. Its origin was first used in academic writings, teaching, then society meetings and conferences developed to exploit the field as a new wave of teaching took hold. As the term entered the workplace in the late 1980s early 1990s, there was an attempt to build ethics into the foundation of corporations in the form of ethics codes, ethics officers, ethics committees and ethics training. This ethics adoption apparently broke down in the early 2000s. The cause, we believe, can be directly attributable to Wall Street's hue and cry for public corporations to either make or exceed their sales, revenue and profit margins each and every quarter/year. Corporate executives were measured on meeting or exceeding their goals, and were handsomely rewarded with huge salaries, huge stock options, and corporate perks.

Now, almost every day when we pick up and scan a local or national newspaper, we can not help but read about the Enron's, Tyco's, Adelphia's, Worldcom's, Healthsouth's, to name a few, and their high powered Ivy schooled [many with MBA's] leaders, Dennis Kozlowski, Mark Swartz, John Rigas, Ken Law, Jeff Skilling, Andrew Fastow, et al. The question we ask, 'What caused these powerhouse executives to do what they did', i.e. caused major corporate bankruptcies, put hundreds of innocent people out of work, many currently still unemployed, with lost pensions and benefits, stockholders loosing billions of dollars of their retirement nest

eggs, and most importantly, the Government spending millions of dollars in man-hours and resources, to research, investigate, prepare for trials, and to prosecute, which in many cases have taken upwards to 8-12 months to conclude. In fact, several have ended in mistrials [mostly through lack of experienced personal to do detailed research], therefore, requiring the litigation process to start over. Certainly, these expenditures, resources and manpower could have been put to work in a more productive pursuit in areas that would benefit the American public in general.

Arianna Huffington, in her current [2003] book, 'Pigs at the Trough', Crown Publishers, lays the foundation for our current situation, in a sort of light humor, by detailing the destructive power our corporate leaders have and how it was used to bring shame to our country.

Based on the various definitions for ethics, ethical, morality and moral law described above, one can readily deduce that the indicted and yet to be indicted, corporate leaders of American business have, as a minimum, violated our trust and breached at least one of the aforesaid cannons, if not all of them. All, however, is not lost. Business Ethics Magazine [www.business-ethics.com], who has been publishing the year's "100 Best Corporate Citizens" for the past 6 years, have indeed found another 100 good doers for the current year 2005. Firms are rated on eight basic categories: (1) total return to shareholders, (2) community, (3) diversity, (4) employees, (5) environment, (6) human rights, (7) governance [added this year by KLD Research & Analytics in Boston, the social data provider for this list], and (8) customers.

There are a lot of resources and information available on the web and elsewhere, on the subject of ethics, that our corporate leaders can take advantage of for self-education on the subject. Recently a new non-profit organization, called 'Open Compliance & Ethics Group' [OCEG, @ www.oceg.org] was formed by a coalition

of leading public companies with the express objective to help and support companies with their governance and compliance activities. Other important organizations involved in providing ethics guidance to companies are: the 'Ethics Resource Center [www.ethics.org] and Business Ethics [www.businessethics.ca], a Canadian resource for business ethics. Academia is also contributing to the cause. The Harvard Business School has had in place for some time an ethics program. Curry College [also located in Massachusetts], recently announced that it is adding a new MBA program in the fall focusing on ethical leadership in corporations. Other major [and minor] academic institutions, I'm sure, have also instituted various ethics programs or will shortly follow suit. Professor Manuel G. Velasquez has published over the years a series of excellent teaching guides; his latest Fifth Edition 'Business Ethics: Concepts and Cases' [2002], Prentice Hall, now has a new exclusive Companion Website™* [www.prenhall.com/velasquez] that provides a variety of learning and teaching tools and models. All these resources are excellent tools for both are current and future business executives and, if used, should help to prevent a future ethics crises.

*Companion Website is a trademark of Prentice Hall.

Officer and Director Responsibility and Liability

The powers, duties and responsibilities of company officers and directors are normally granted under a state's business incorporation statute, as well as by the company's bylaws, including other applicable state laws. Likewise, the powers of a corporation are also granted under same statute. Additionally, certain federal laws also apply to corporations on a general basis, and various federal agencies, such as the Securities and Exchange Commission [SEC] have rules and regulations that apply to public companies. Up until the enacted of Sarbanes-

Oxely, federal laws, for the most part, apply only to corporations and did not directly impact officers and directors.

Let's then examine the powers, duties and responsibilities of officers and directors as they relate to ethics and compliance in the workplace. A director or officer who performs his duties in good faith and in a manner he/she reasonably believes to be in the best interests of the corporation and with such care as an ordinarily prudent person in a like position would use under similar circumstances will normally have a complete defense to liability. A director or officer will also be entitled to reasonably rely on information, opinions, reports or records presented by other company officers, employees or board committees, including inside and outside legal counsel, accountants, investment bankers, etc., as to matters which the director or officer reasonably believes is within such person's professional or expert competence. An incorporator or officer could, under most circumstances, be liable to shareholders for signing false articles of organization, amendments, improper stock issuances, or any consolidation and merger documents. Normally, a director who has voted to authorize an unlawful dividend or other distribution to shareholders will be jointly and severely liable to the corporation.

Some state statutes allow statutory indemnification by the corporation of both officers and directors for losses and expenses incurred in connection with any matter in which such person acted in good faith and in a manner he/she reasonably believed to be in the best interests of the corporation. A director against whom a claim is successfully asserted with respect to an unlawful dividend, stock purchase or stock redemption is entitled to contribution from the other directors who voted for such action

Most state statutes also have a so called ‘Business Judgement Rule’ which states that in making a business decision, the directors of a corporation are presumed to have acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the corporation. A party contesting such action has the burden to rebut the presumption. Directors, at all times while serving as a director, have a duty of ‘utmost good faith’ to the corporation and its shareholders. Directors must review all material information reasonably available to him/her, then act in an informed and deliberate manner in determining whether to approve a transaction. The general standard applied to directors is one of ‘gross’ negligence, which is a higher standard than that normally applied to other situations. If evidence shows that directors acted out of self interest or are engaged in self dealing, the burden then shifts to the director and requires the director to establish that the transaction was fair and in the best interests of the corporation and its shareholders.

In cases where the Business Judgement Rule doesn’t apply or is inapplicable, there is a presumption of a ‘Duty of Loyalty’ to the corporation. For example, where a director stands on both sides of the transaction as a director of the parent and the parent’s subsidiary and participates in any decision making, that director has the burden of establishing the entire and complete fairness of the transaction. Even when the decision was approved by a majority of the [independent] directors or ratified by an informed vote of shareholders, the entire fairness standard governs. In that situation, the shareholder challenging the transaction has the burden of proof.

In case where the Business Judgment Rule or the Duty of Loyalty do not apply or are not applicable, there is always the presumption of a ‘Duty of Care’. For example, directors can rely on experts or professionals who have been selected with reasonable care**,** including [certified] public accountants, lawyers and investment bankers, as well as on reports made in good faith by officers and independent consultants. Directors cannot

proceed hastily or accept representations without scrutiny, or fail to seek out other critical information, as applicable. It is extremely important the board minutes be well document. This does not mean that detailed minutes are necessary, but it is important to detail the important issues considered in approving 'material' transactions. Minutes are presumed to be correct, unless proved to contrary with detailed evidence.

It is clear from the above that officers and directors already have, as a minimum, a duty of loyalty and due care to the corporation and the shareholders. Additionally, most senior company executives [Chairman, President, CEO, CFO, etc.] are also under a written employment agreement. So it would appear, in the author's opinion, that officers would [could] also be liable for a breach of contract action. Directors are, in most cases, appointed as such under a written contractual arrangement, either a formal agreement, or a 'Memorandum of Understanding' or a 'Letter of Understanding', etc. That means they may also be liable under a breach of contract theory [see Veil Piercing below]. It would also appear then that under state statutory requirements, coupled with the company's bylaws, we have had, and continue to have, sufficient controls to ensure total and complete compliance with corporate governance matters. In fact, Massachusetts, on July 1, 2004, implement a complete new Business Corporation Act, M.G.L. [Massachusetts General Laws] 156D. This new statute has more teeth to it as it relates to corporate governance and personal officer and director liability. It completely replaced the old law [M.G.L. 156B] statute, and all new, as well as all exisitng corporations, are now governed by the new 156D statute.

Corporate Governance and Compliance Under Sarbanes-Oxley

Although we have had adequate state statutes regarding officer and director responsibilities and duties, the demands of Wall Street, and the personal greed of certain of our corporate leaders, the federal Government had to step in and enact Sarbanes-Oxely, which provides for new and more stringent rules and regulations mandating governance and compliance, over and above the standards enumerated above. SOX also impacts officers and directors personally. As SOX is a very detailed and complicated statute it is not the intent of this paper to provide a detailed explanation of all the Act's requirements. Suffice it to say, that section 404 is probably one of the more critical sections that have caused the most concern and expense. This section deals with internal controls and has had the most impact on the business. As stipulated by section 404, the SEC was required to adopt rules regarding internal controls, and further requires that a company's independent auditors attest to and report on management's controls assessments, following standards established by PCAOB [Public Company Accounting Oversight Board, www.pcaob.com]. In a nut shell, the basic SEC rules requires that management's annual internal control report contain, as a minimum, the following: (1) assessment and framework for evaluating the effectiveness of the company's internal controls; (2) managements commitment and responsibility for establishing and maintaining proper internal controls; and (3) the company's auditors must issue an attestation on the company's assessment initiatives. Needless to say, a company's internal control systems must be revamped to include assurances of accurate records maintenance, as well as financial reporting that complies with generally acceptable accounting principals. Under the current deadline established by the SEC [Nov 15, 2004 for 'accelerated filers, i.e. companies with a market cap of over $75 million], the company's most senior manager must certify that the company's internal controls comply with the new Act. All other companies have until June 15, 2005 to make the certification. Also, under the new rules [303A] 3

signification rules emerged: (1) the need for listed companies to have a majority in independent directors, (2) a tightened definition of what constitutes an 'independent director, and (3) guidelines when a director is not 'independent'.

The old cliché 'Let the Buyer Beware' or for private companies under the Act it could be called 'Private Companies Beware and Be Worried'. Under certain circumstances, a private company could also fall under the Acts requirements. For example, companies dealing with the federal Government and/or various Governmental agencies, such as: 'Environmental Protection', 'Federal Communication Commission', 'Federal Trade Commission' to name a few, would be required to comply with certain aspects of the Act. The 2 most critical areas that a private company must be concerned with are: 'Documents and Records Retention', and 'Whistle-Blowing'. It is also recommended that private companies also implement a 'Business Code of Ethics' policy [see appendix I].

In-House Corporate GC's [General Counsel] are currently also facing an instant headache. A thorny but important question currently facing GC's is that of 'Attorney-Client Privilege' as it relates to providing outside auditors confidential auditing information in order for them to comply with the requirements of the Act. In response to this new dilemma, a new Corporate Counsel Consortium [CCC] was formed by several major corporate GC's in 2004, headed by Viacom's VP/General Counsel, Mike Fricklas. In an attempt to address the issues in a uniform and consistent manner without violating or wavering the sage old 'Attorney-Client Privilege' doctrine, and at the same time be responsive to the ACT, CCC is proposing to implement standard [non-binding] guidelines for GC's to follow. CCC's activities are being coordinated by attorney David Brodsky, a partner at the law firm of Latham & Watkins. CCC, acting as a 'lobbing' group, has established as its primary

major objective, to prepare new federal regulations to address these issues. In fact, attorney Brodsky has already delivered a report on the accounting issues to the American Bar Association's midyear meeting in February, and plans to address ABA's next annual meeting in August. In the meantime, CCC's present position is to have GC's provide non-privileged documents, but not to with hold other pertinent [privileged] documents deemed necessary by the auditor.

Needless to say, implementing a compliance solution must be made a high priority for all public companies and Part II of this paper provides guidelines and an implementation strategy and procedures necessary to successfully to that, hopefully, with a minimum pain threshold and expense to the company.

Remedies for Redress; Veil Piercing

A basic understanding of the underlining theories of liability would be helpful to fully understand and appreciate the rights and remedies available for a committed wrong. Liability is an all-encompassing legal term which can be defined simply as 'a condition of being responsible for either an actual or potential loss that can result from an action of tort or contract'. A tort is a private or civil wrong or injury founded upon negligence, strict liability or intentional misconduct. It is a legal wrong committed upon a person or property independent of contract and arises by operation of law. A contract action, on the other hand, arises from a breach of an agreement between two or more parties, based upon sufficient consideration to do or not do a particular thing.

The most predominate legal theory for bringing a lawsuit is 'negligence'. Negligence is defined as "The omission to do something which a reasonable person, guided by those ordinary considerations which ordinarily regulate human affairs, would do, or the doing of something which a reasonable and prudent person would not

do" [Black's Law Dictionary, Revised Fourth Edition, 1968]. There are several degrees of care, ranging from 'Ordinary Negligence', 'Wanton Negligence' 'Wilful Negligence' to 'Gross Negligence', but there is no legal degree of negligence, per se. Classifying negligence under one of these degrees of care only indicates the special duty of care an individual can be held to. To prove negligence, an individual must show that the other person owed him/her a duty of care to act or refrain from acting in some manner. The question then becomes for the judge and jury how great was that duty and care, and, therefore, the resulting remedy and damages.

As indicated previously in this paper, many companies [the 'Parent Company'] form separate independent companies [generally referred to as 'wholly owned subsidiaries/divisions'], or other business or legal entities, which are located either in the US or off-shore. In most instances, these independent companies are formed for a very legitimate business purpose. Some, however, are formed to handle the 'cooking' of the parents' books and records, in a deliberate attempt to immune the parent, and their officers and directors, from liability. Generally these subsidiary companies are viewed by the courts as a distinct legal entity, separate and apart from the parent, and their officers, directors and shareholders, so long as the corporate characteristics of (i) centralized management, (ii) free transferability of interests, and (iii) continuity of life are, at all times, maintained. The courts, absent fraud, misrepresentation or torts, will generally insulate the parent and its officers, directors and shareholders from personal liability and their own personal assets. Limited or no liability is the general rule and not the exception.

The doctrine of veil piercing, or as its more commonly referred to 'Piercing the Corporate Veil', is a little known and rarely used remedy to reach the assets of either a parent company and/or their officers and directors personally. It is employed by courts in common law countries [such as the US and England] and in civil law

countries, who use the system of dependency on statutory law. Most, if not all, US federal and state courts recognize veil piercing. Both courts require some sort of wrongdoing or fraud before the corporate veil can be pierced. Several federal courts have developed and applied a 'Federal Common Law' of veil piercing that allows for more easy piercing than do state courts. In foreign jurisdictions, especially civil law countries, the system of depending on the country's statutory law, has made the law of veil piercing even more uncertain than that employed by US federal and state courts. Therefore, the moving party should and must do a through analysis of each situation in order to determine the best venue to file suit in.

Frederick J. Powell, in an effort to formulate clear veil-piercing rules, in his 1931 treatise, 'Parent and Subsidiary Corporations: Liability of a Parent Corporation for the Obligations of Its Subsidiary', laid down three tests, all of which must be met, for piercing the corporate veil: the first test, the "alter ego," or "mere instrumentally" test, requiring that the subsidiary be completely under the control and domination of the parent, the second test is the "fraud or wrong or "injustice" test, requiring that the defendant parent's conduct in using the subsidiary have been somewhat unjust, fraudulent, or wrongful towards the moving party [Plaintiff], and the third test, the "unjust loss or injury" test, requiring that the moving party actually has suffered some harm as a result of the conduct of the defendant parent. Powell, in an effort to assist courts in determining when the 'alter ego' test is satisfied, also formulated a 'laundry list' of questions the courts should ask themselves. These questions include whether:

(1) the parent and the subsidiary have common stock ownership;

(2) the parent and the subsidiary have common directors or officers;

(3) the parent and the subsidiary have common business departments;

(4) the parent and the subsidiary file consolidated financial statements and tax returns;

(5) the parent finances the subsidiary;

(6) the parent caused the incorporation of the subsidiary;

(7) the subsidiary operates with grossly inadequate capital;

(8) the parent pays the salaries and other expenses of the subsidiary;

(9) the subsidiary receives no business except that given to it by the parent;

(10) the parent uses the subsidiary's property as its own;

(10) the daily operations of the two corporations are not kept separate; and

(12) the subsidiary does not observe the basic corporate formalities, such as keeping separate books and records and holding shareholder and board meetings.

Under Powell's theoretical questions, he did not indicate and/or stipulate that all of the above questions must be answered affirmatively, but left it to the courts to decide the weight to be given to each and the number of affirmative yeses, to allow the veil to be pierced. As veil cases started to appear, other questions related to Powell's second theory test evolved, such as: (1) did the parent use the subsidiary to commit a tort, (2) did the parent use the subsidiary to engage in misrepresentation, (3) did the parent's use of the subsidiary amount to actual fraud or violation of a statute. These questions seem to go directly to the heart of our classic 'cook the books' case made earlier, and, in the author's opinion, makes for a good case against the officers, directors and shareholders personally of the now bankrupt companies, which are without any assets to attach.

Veil piercing, in summary, is directly dependent on the courts total assessment of the facts in each case after applying the now established guidelines i.e. the parent's complete domination of its subsidiary, including its finances, operations, etc., and was the subsidiary merely a conduit of the parent, and the parent used the subsidiary to perpetuate a fraud or injustice, or otherwise circumvented the law.

Part II: Compliance System Architecture

This section of the paper will focus on the management perspective of building and sustaining a compliance initiative. We will focus on a systems approach to achieve transparency. Our goal is not to recommend a specific vendor configuration, but to highlight the significant components which together will help organizations to sustain compliance.

The main purpose of Part II is to outline the major elements of a program that will help to carry out top management policy for running a compliant enterprise. Through out this section, we assume that corporate leadership intends to comply with the intent and spirit of the Sarbanes-Oxley law, and not just provide the appearances of compliance. There is a significant difference, because true compliance means changing many of the traditional ways of working in order to achieve transparency, audit ability, and accountability. It also requires leadership, a commitment from all levels of management, as well as, vision, and a willingness from middle management to operate a transparent organization. Given these characteristics, there is a systemic approach to managing the requirements for enterprise compliance in order to ensure ongoing sustainability and agility. A sincere commitment to compliance will enable the following iterative approach to be instituted:

1. A frank and collaborative assessment of enterprise risk is performed;
2. Competitive, market, and internal threats are prioritized;
3. Risk mitigation strategies are defined;
4. Internal controls for financial reporting are evaluated;
5. A requirements management process is put in place;
6. Business processes are modeled;

7. Key decision points are documented; and,
8. The artifacts of the compliance initiative are preserved.

In order for this approach to take root in the rank and file, management's attitude towards regulatory compliance must be projected by thought, word, and deed. The "tone at the top" is the motto of the Institute for Internal Auditors; it refers to the posture of senior management with respect to regulatory compliance, and how this is perceived in the organization.

The Tone at the Top

If a company existed merely to comply with Sarbanes-Oxley, life would be much easier for Chief Compliance Officers. Corporations do not exist, however, merely for the sake of complying with regulatory agencies. In a speech to corporate executives, Lori A. Richards, Director of Office of Compliance Inspections & Examinations for the US Securities and Exchange Commission (SEC) , suggested that:

> *"…the culture of compliance must be a part of a company's core business model, yet the compliance framework must be connected to the strategic goals of the corporation in order to transcend current levels of business discipline".*[1]

In other words, companies need to foster a new way of thinking about the regulatory environment so as to integrate the organization's business discipline with compliance activities. Getting it right means that compliance does not have to be at odds with other corporate goals. Moving towards a transparent organization can greatly benefit the business. According to the Financial Times:

"A study of more than 2500 international companies found the Sarbanes-Oxley act and other reforms implemented following recent scandals had succeeded in improving the relative performance of large US companies by more than 10 percent."[2]

Thus, the "culture of compliance" that Richards promotes will merge operational decision-making with ethical principles grounded in the spirit of Sarbanes-Oxley. Compliance requires transparency, meaning that no significant risks or facts are hidden from the investor. In the final analysis, transparent organizations are high performing organizations because they have superior understanding and control of financial reporting, customer service, supply chain, performance management, and other corporate systems. A transparent enterprise is agile; it can adapt quickly to new opportunities and threats as well as to new regulatory pressures.

Moving from regulatory mandates to changes in processes and behavior requires the formulation of policies that spell out the responsibilities of departments and individuals throughout the organization. Writing corporate policy that is consistent, uses a controlled vocabulary, and abides by a certain semantic rules is an effective and efficient means of bridging the management and system worlds. Software industry associations such as the Object Management Group [OMG] are currently in the process of designing standard methodologies and tools for the regulatory domain. These standards will be based on stable technologies such as extensible markup language [XML] as well as evolving computer idioms such as business process execution language [BPML]. The goal of these emerging standards is to be able to distill corporate policy

---

[1] Lori A. Richards, "Speech by SEC Staff: The Culture of Compliance", April 23, 2003, Tucson, Arizona

into a set of precise statements that can eventually be compiled into executable computer code. Although these technologies will facilitate management oversight, they will not replace the tone at the top of the organization.

Risk Management

Risk management has been elevated to a high priority exercise at all levels of the corporation. Collaboration amongst managers and stakeholders is paramount if different kinds of risk are to be identified.

Sarbanes-Oxley requires that companies identify events of conditions that may occur in the future, which will have a negative impact on financial projections. These risks stem from a variety of internal and external forces, such as:

- Loss of key personnel,
- Worldwide market conditions,
- Competitive threats,
- Supplier difficulties,
- Large contract terminations, and of course,
- Risk of regulatory non-compliance.

The set of risks will be different for each company. Tools for assessing risk using sophisticated mathematical models are maturing. They can help to quantify and objectify the ranking of risks using a collaborative, voting

[2] "Financial Times", September 7, 2004, page 1

approach. Brainstorming and informal ranking on Excel spreadsheets suffices for most companies. No matter how it is accomplished, risks need to be identified and prioritized with respect to other corporate goals and objectives. A mitigation plan needs to be established to detect, if not prevent, fraudulent use of corporate assets. These plans become another kind of corporate policy.

Internal controls are essential for ensuring that corporate policies are followed. Of all the possible systems and processes where internal controls can be implemented, which ones do you tackle first? Enter risk management. Although the risk management techniques are not new, Sarbanes-Oxley has elevated the importance of formalized risk management. Ignorance of risks cannot be an excuse, therefore it is incumbent on management to identify and prioritize risks that may affect financial performance. Under Section 409 of Sarbanes-Oxley, management must disclose any risks that are significant enough to possibly affect future financial performance, and it must do so rapidly. In the words of the statute:

> "Each issuer reporting under section 13(a) or 15(d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest.".

What is a material change? It depends totally on the impact on the bottom line. What is material for mid-sized company may be insignificant for Wal-Mart. Management might want to describe a set of rules to create a

quotient for each risk, so that if the risk does become an issue, the compliance team will know how to respond. Ideally, the risk rules will be incorporated into the business process, so that a material event will trigger the appropriate notifications and disclosures. It is important to remember that risk management is a process which must be documented and adaptable to the changing economic conditions of the enterprise. An attitude of remaining silent about known risks is unacceptable and may be interpreted as fraudulent. To the extent that uncovered material risks are not identified, management is exposed to penalties for non-compliance. Emerging technologies can also help with the rapid disclosure requirements of Sarbanes-Oxley. Business Process Management [BPM] software lets organizations sequence and rearrange the steps in a business process. The disclosure process itself can be orchestrated as a sequence of activities that will alert the compliance team whenever a potential material risk is realized. Rules can be programmed into a core business process to recognize a material threat, for instance, the price elevation of a commodity. The core business process can then trigger the disclosure process, which will notify members of the compliance team of the threat. The risk quotient of the threat can be re-evaluated, and a restatement of quarterly financial projections can be re-calculated using Extensible Business Reporting Language [XBRL], another emerging technology. Having this disclosure process in place gives peace of mind to the Chief Compliance Officer, and whenever the disclosure process is triggered, an audit trail is left behind.

Internal Controls

Internal controls mitigate risks by detecting or preventing fraud. There are general controls that apply to a wide range of activities and there are application controls that are specific to a system or business process.

Industry associations have produced frameworks to help organizations get started with the evaluation of internal controls.

Internal controls are the mechanism by which management verifies that corporate policy is being followed. With respect to Sarbanes-Oxley, the emphasis is on internal controls for financial systems reporting. Section 404 introduces the idea of an "internal control structure" but fails to define it. It is left up to management to decide what controls should be in place, to prioritize where to place controls, to test and document them, and to assess their effectiveness. Recently, several industry initiatives have been established to create a body of knowledge regarding risk management and internal controls. The most important of these initiatives are the Council of Sponsoring Organizations [COSO] and Control Objectives for Information Technology [COBIT®][3].

COSO is an attempt to provide guidance to the financial reporting community. The Council of Sponsoring Organizations for the Treadway Commission, originally formed in 1985 as part of the National Commission on Fraudulent Reporting, has recently updated their publications on risk management. COSO, or the newer version COSOII, is a framework for establishing, monitoring, evaluating and reporting on internal controls regarding the financial processes of an enterprise. COSO defines five essential features of an effective internal control system:

- **Environment -**Establishes the "tone at the top", and institutes the idea that internal control is taken seriously by senior management. If the strategic business environment is not controlled, all other

[3] COBIT is a trademark of the Information Systems Audit and Control Association, Rolling Meadows, Ill.

internal controls are doomed to failure.

- **Assessment** – Assessment of system risk such as data security, availability of information, and analysis of business and individual performance;

- **Activities** – The policies, procedures and practices that are put into place to ensure that business objectives are met and risk strategies are followed.

- **Communication** – The mechanism by which risks are managed and internal control policies are disseminated;

- **Monitoring** – The oversight of internal controls and risks by adapting continuous process improvement techniques.

COSO raises the consciousness and offers a practice discipline for Enterprise Risk Management [‘ERM’]. For companies struggling to get started with Sarbanes-Oxley compliance, it provides an important overarching control strategy that can serve as a template for moving forward. COSO provides food for thought for the compliance team and it prepares them to ask management, line, and staff the right questions.

The Treadway Commission, however, did not address specific technology concerns like infrastructure, or software development. Yet, computer systems provide the data from which financial reports are made in all

publicly traded companies! How can there be internal controls without information technology controls? Auditing texts such as Auditing: Principles and Procedures, by Arthur Holmes, had not been significantly updated in decades. Clearly, there was a need to update internal control theory and practice for the millennium.

To bridge the gap between IT controls and financial controls, a best practice framework was invented by IT Governance Institute. While COSO focuses on business level activities, COBIT® drills down into the supporting IT activities. COBIT® is a methodology product that formalizes accepted international standards for best practices of IT controls for applications and enterprise-wide information systems. COBIT® is technology independent.

COBIT® defines control objectives in four IT domains:

1. **Plan and Organize** – Set the tactics and strategy for the project.
2. **Acquire and Implement** – Acquire and maintain technology and manage change.
3. **Deliver and Support** – Define and maintain service levels.
4. **Monitor and Evaluate** – Provide management oversight, assessment, and auditing.

COBIT® is best thought of as a reference model rather than a prescribed set of processes to implement verbatim. The idea is to implement the best practices that support the control objectives defined in the reference model, rather than trying to implement the reference model itself. In objected oriented[4] terms, COBIT® is an abstraction and each subscribing company ought to create an instance of it to fit their specific

risk profile. COBIT® offers more than 300 general and application control objectives. General control objectives address issues such as data security, access to restricted area, methodology, personnel evaluation, and other management and operation considerations that span across enterprise systems. Application control objectives, on the other hand, address particular system issues such as vendor control, separation of duties, and checks and balances. Application controls can usually be integrated with the software application itself. In fact, millions of dollars are being spent by corporations today to identify internal control weaknesses in existing systems and to remediate them. This is very labor intensive and requires highly skilled software experts.

Two more emerging technologies offer assistance for the problem of expensive internal control remediation: rule engines and activity monitors. Business rule engines, or inference engines, refer to a technology that has evolved from the field of artificial intelligence. They use pattern matching algorithms to identify business rules that are relevant to a given set of data. Upon request, the rule engine can make an inference which is in effect a decision that directs the flow of software execution. For instance, a business analyst may stipulate a set of rules regarding the authorization of invoice payments. The rule engine can "decide" whether or not to approve the invoice based on the set of rules. The major benefit of the business rule approach is that the rules can be changed without changing the software of the underlying business process. Management can change the rules to loosen or tighten the internal control mechanism to meet changing regulatory conditions. Business rule engines work hand in hand with business activity monitors [BAM]. A business activity monitor is a layer of software that filters transactions such as trade executions. In today's compute intensive

[4] Object oriented is a methodology that system designers use to classify real world things into concepts that can be manipulated by software.

enterprises, financial transactions are transmitted via messages that are routed between buyer and seller. BAM software can be programmed to intercept these messages and pass them on to a rule engine for internal control evaluation. If the transaction meets internal control tests, then the transaction is allowed to continue otherwise it is aborted and routed to the attention of the audit staff.

With or without of emerging technologies, the major benefit of the COSO and COBIT® frameworks are to help the Chief Compliance Officer ask the right questions of his or her C level peers. Using these frameworks, you can perform an initial assessment of your strengths and weaknesses with respect to risk management and internal control. Then you can develop a customized action plan to build and sustain regulatory compliance.

The Need for a Compliance Information Architecture

Corporate governance policy must be translated into enterprise business requirements. Information systems play a crucial role in ensuring transparency. Management control goes beyond information systems which are really meant to support accounting imperatives and personnel reward incentives.

As the Chief Compliance Officer for the corporation, you have done your due diligence and uncovered strengths and weaknesses in how your company identifies and mitigates risk. You have also identified opportunities for fraud in your financial reporting systems and business operations. Now what? If you are a consultant, perhaps your job is done, but as a manager, you have the responsibility for putting into motion a program to manage and sustain compliance. Your program has to be good enough so that your CFO and CEO

can attest to the veracity of your internal control structure. How can you be sure that your program will produce these results?

During your COSO and COBIT® assessment, you identified areas of concern that need to be addressed in accordance with the Sarbanes-Oxley regulation. Perhaps one weak area is the purchasing process. You've noted that there is not sufficient separation of duties between accounts payable and vendor management. Consequently, you've expressed a control objective to eliminate the opportunity for fraud in the invoice payment process. This objective will be written up as a policy which will be enforced by establishing an application level internal control in the accounts payable software system. Your internal auditor will develop a test to measure the effectiveness of the internal control. This is the correct approach. Multiple this example by many thousands of control objectives and you begin to get a sense of how overwhelming it can be to create an internal control system. There is too much information to fit into you head, unless you are running a very small company. What you need is an architecture to manage the information, so that you can map each regulatory item into relationships:

- Regulation to Policy;
- Policy to Control Objective;
- Control Objectives to Internal Control;
- Internal Control to Test Case;
- Test Case to Test Results.

Correlating this information is the basis of a regulatory compliance architecture. Unfortunately, once you perform this initial mapping of information, it will change! Business conditions will identify additional risks that need to be controlled. New regulations may be thrust upon you. From an external auditing perspective, you will be asked to demonstrate that the risk management plan is in place using specific internal controls that have been tested. Because auditors always are looking back at historical transactions, your compliance architecture must be able to reconstruct the state of your internal controls as of a certain point in time.

Information mapping alone is not sufficient to manage and sustain compliance. You need people to take custody of policies, control objectives, internal controls, and test cases, and test results. People make compliance happen, so you should associate each regulatory item with an individual or department owner. Ideally, the personnel performance appraisal and reward system will take into account the individual's compliance responsibilities.

Developing the compliance architecture may sound like a lot of work, and it is, but without it you will be recreating the same set of regulatory information year after year. In the long run, it will cost you more to take an ad hoc approach to managing these data. To sustain the regulatory effort going forward, and to be able to respond to a fluid regulatory environment, you need compliance information architecture.

Components of Compliance Information Architecture

A compliance information architecture is independent of any vendor platform. No single vendor has a complete solution. Requirements management, modeling, and configuration management each play a role. Emerging technologies can accelerate the push for sustained compliance.

Go to any trade show where Sarbanes-Oxley is discussed and you will be overwhelmed by vendors claiming to have the solution to your problem. The truth is that compliance architecture is not realized by a turn-key application; rather you need a combination of processes and software that can evolve with changing business conditions.

The core component of compliance architecture is a requirements management system. Your assessment of risks will result in a set of enterprise requirements which may be expressed as policies, control objectives, internal controls, or test cases. A requirements management system will enable you to define types of requirements and trace them to each other. This feature is perfect for performing the information mapping discussed previously. Unlike common desktop applications such as Excel and Word, a requirements management system will also track changes to a requirement over time, so that any re-statement of the control objective, for instance, will be recorded. Also, a requirements management system will let you set characteristics of the requirement, such as priority, responsible department, planned implementation, and more. Three mature requirements management products are CaliberRM from Borland, DOORS from Telelogic, and RequisitePro from IBM.

Another indispensable component of compliance architecture is a business modeling capability. Business modeling lets you describe your business processes from a high level. Most people find it easier to comprehend

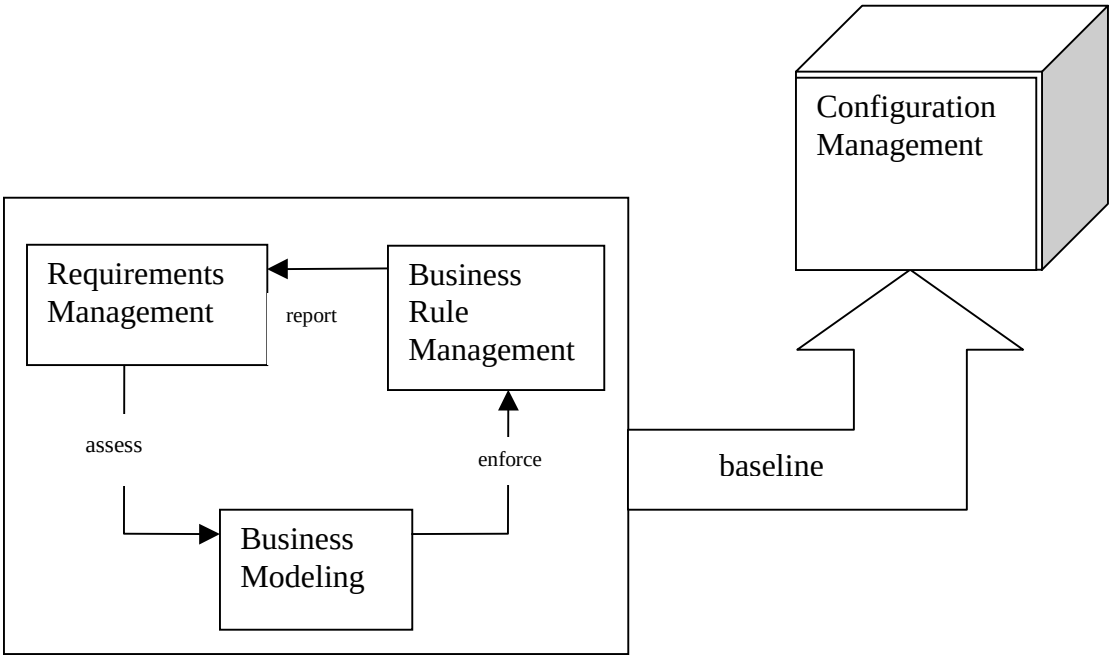
a sequence of events and decision points using visual diagrams rather than purely textual descriptions. Using visual modeling techniques, managers can understand the big picture and yet be able to drill down to details when necessary to explore trouble spots. Business modeling can be achieved using the basic flowchart symbols of rectangles, arrows, and diamonds available in inexpensive desktop applications. More advanced organizations might want to use more sophisticated tools that are based on emerging standards such as Business Process Execution Language (BPEL). What ever tool you use, the important result is to understand and document the steps in key business processes, especially for financial reporting. You cannot control what you don't understand. Recording your processes as a visual model will be sure to yield several exclamations of "a-ha, so that's how it works!" amongst management and staff.

Configuration management is another core component of compliance architecture. These systems are well known in the software development community but not amongst auditors. A configuration management systems stores and associates many pieces of information and is able to reconstruct a system state as of a certain point in time. That is just what you need in order to demonstrate what the internal controls were when the company issued the 10-K report. Configuration management systems can be extremely expensive and complex, but most companies will do fine with lesser expensive, basic systems like Visual Source Safe from Microsoft, or even the free, open source code versioning system known as CVS.

A business rule management system is another key component of your compliance architecture. Business rules are the decision points in your business model. They determine the direction of your business flow, and they enforce management policy. When should customer credit be rejected? What price should be proposed to our government customers? Can a trade be executed at midnight if the security is traded on the NYSE and in Hong

Kong? These are all examples of operational decisions upon which internal controls can be placed. In compliance management architecture, there is a direct link between these minute decisions and the guiding regulation. If the regulation changes, you can modify the decision logic appropriately, if you know where it exists. Your rule management system will identify where decisions are made in the enterprise, whether it be in software, manual process, or in the heads of experts. A good rule management system will categorize your business rules along many dimensions cluster them according to function. It dovetails and complements your requirements management system.

Figure 1: Compliance Component Architecture



Other than the core components shown in figure 1, several new technologies that can foster compliance are emerging into common usage. These include:

- Business Process Management,
- Business Rule Engines, and
- Dashboards.

Business Process Management, or BPM, builds upon distributed computing services to enable business events to be linked in the optimal workflow. For instance, consider what happens when you place an order for a book on a web site. First the system searches inventory to see if the book is in stock, then you place the book in the shopping cart. When you checkout, you credit card information is collected and validated real-time with the credit agencies. Next you pick the shipping method: normal, 2-day, or next day. Finally your card is credited with the purchase, and the order is queued for picking. Each of these steps is an event in the order entry business process. With BPM software, you can rearrange this sequence with minimal effort, or add an additional step, such as determining whether a stock replenishment point has been reached. Why is BPM important to regulatory compliance architecture? Because steps can be added to financial reporting business processes, for internal control execution, notification of unusual events and other real time monitoring that is suggested, if not required, by Sarbanes-Oxley.

Business Rule Engines have matured to become a viable tool for many industries to quickly adapt to regulatory and competitive changes. Originating from research into artificial intelligence, business rule engines make inferences based on facts and if-then statements that have been defined by management. Consider all the factors that lead to a pricing decision in a retail store:

- Customer purchase history,
- Customer credit history,
- Product promotion,
- Coupons,
- Complementary products in the shopping cart,
- Etc.

These pricing rules need to be organized and prioritized so that the same decision is reached each time for the same set of facts. Rather than implementing this logic using programmers in the traditional software release cycle, business rule engines let the business owner modify the rules. This provides for much greater flexibility and faster turnaround time. For the compliance officer, business rule engines offer the luxury of inserting, removing, or modifying internal control logic. Note that you don't need a business rule engine to mange business rules; however, the technologies complement each other. In fact, the software industry is starting to adopt standards for the translation of policy statements into executable business rules. The RuleML initiative[5], for example, is an emerging standard that lets compliance officers and business people stipulate corporate policy using a controlled vocabulary and semantic constraints. Once the policy is written in the RuleML standard, conversion software can be invoked to translate the policy into a rule that can be executed in several commercial and open source rule engines.

[5] http://www.ruleml.org/

A Dashboard can help managers cope with more and more information. Dashboard is the name given to a technology that lets a manager focus on exceptions using iconic representations of information such as stoplights and gauges. Dashboards can be employed, for instance, to get an instant appraisal of how well risk is being managed in financial reporting. Assuming that relevant risks have been identified and prioritized, you can program a dashboard to report on how many controls have been established to mitigate the risk, and whether or not these controls have been tested successfully. Success with dashboards depend on having an underlying compliance architecture with meaningful data with respect to control objectives, internal controls, requirements, tests, and other regulatory information items. You also have to report on the right metrics. Although certainly not the first component to implement in your architecture, dashboards can help facilitate the reporting and monitoring aspect of sustaining a compliance effort.

The Bright Side – Benefits of Good Governance

The effort to become compliant with Sarbanes-Oxley, at first glance, seems to be enormously painful with few benefits. Assessing and documenting risk, mapping requirements to control objectives, testing internal controls: these activities take time and expertise – precious resources that could be applied to pursue other opportunities. On second reflection, though, you can appreciate that the disciplines required to be compliant are also those needed to be agile in a completive environment: modeling your business processes, managing business rules, and managing requirements. Since you have to become compliant with Sarbanes-Oxley anyway, you might as well do so in a way that will benefit your business long term. By embracing the spirit of Sarbanes-Oxley to become a transparent organization, you will gain the respect of your shareholders, employees, and other business partner and corporations. Despite the initial pain and expense, compliance disciplines will foster

greater corporate agility and competitiveness. Through the concerted effort of like-minded managers, you will help restore the faith of investors in our free market, but regulated, economy.

Summary

In summary, as Michael Lissack in his introductory statement so elegantly phrased it and as this essay illustrates, corporate America has been struggling for the past several years with an ethics breakdown in the workplace. This sad chapter, we believe, has finally come to an end. In the short term, the federal regulators stepped in and implemented a very strict governance and compliance statute [Sarbanes-Oxely]. The Act is and continues to be, a major burden on corporate management. In the long term, academia needs to step forward and implement specific detailed ethics programs [in light of our past experiences] and make them mandatory courses for every student, in every program. It is up to tomorrows business leaders to repair the images of our past leaders and to set new examples and directions for ethics in the workplace. This is a wonderful world we live in and we should take advantage of all it offers to us.

Appendix I

Business Conduct and Ethics Policy- *SPECIMEN*

XYZ Company has established this 'Code of Business Conduct and Ethics' which sets out basic principles to guide all employees in its dealings with customers and business partners. It covers a wide range of business practices and procedures; however, it does not cover every issue that may arise. All of our employees must conduct themselves accordingly and should seek to avoid even the appearance of improper behavior. This Policy must also be followed by all officers of the company, including the Board of Directors, as well as all agents and representatives, including consultants, of the Company.

If a law conflicts with a Policy statement you must comply with the law; however, if a local custom or policy conflicts, you must comply with this Policy. If you have any questions about these conflicts, you should ask your supervisor or manager or the Company's in-house attorney/law department how to handle the situation. Those who violate the standards set forth in this Policy will be subject to appropriate disciplinary action. If you are in a situation that you believe may violate or lead to a violation of this Policy, follow the guidelines described in this document.

I. COMPLIANCE WITH LAWS, RULES AND REGULATIONS

All employees must respect and obey the laws of the states and cities in which the Company operates. Not all employees are expected to know the details of these laws, but it is important to know enough to determine when to seek advice from supervisors, managers, legal counsel or other appropriate Company personnel.

II. CONFLICTS OF INTEREST

Conflicts of interest are prohibited as a matter of Company policy. A "conflict of interest" exists when someone's personal interest interferes in any way with the interests of the Company. Conflict situations may arise when an employee, officer or director takes action or has interests that may make it difficult to perform his or her work for the Company objectively and effectively. Conflicts of interest may also arise when a director, officer or employee, or a member of his or her family, receives improper personal benefits as a result of his or her position in the Company. It is almost always a conflict of interest for a Company employee to work simultaneously
for a competitor, customer or supplier. You are not allowed to work for a competitor in any capacity while employed by the Company. The best policy is to avoid any direct or indirect business connection with our customers, suppliers or competitors, except on behalf of the Company.

Conflicts of interest may not always be clear cut. If you have a question, you should consult with higher levels of management or the Company's in-house counsel. Any director, officer or employee who becomes aware of a

conflict or potential conflict should bring it to the attention of a supervisor, manager or other appropriate personnel.

III. CONFIDENTIAL INFORMATION

Employees who have access to confidential information are not permitted to use or share that information for any other purpose except the conduct of the business of the Company. All nonpublic information about the Company should be considered confidential. To use nonpublic information for personal financial benefit or to "tip" others who might make an investment decision on the basis of this information is not only unethical but also illegal.

IV. INTELLECTUAL PROPERTY [COPYRIGHTS, TRADEMARKS AND PATENTS]

The Company is committed to defending its own copyrights, trademarks, logos, and patent rights, and to respecting the valid and enforceable intellectual property rights of others. The Company is committed to maintaining the highest standards of ethical conduct in connection with such intellectual property rights of others. The Company has also adopted a separate Policy entitled 'Policy For Protecting Intellectual Property/Confidential Information' which is also included in this Handbook. All employees must also strictly abide by this IP policy.

V. CORPORATE OPPORTUNITIES

Directors, officers and employees owe a duty to the Company to advance the legitimate business interests of the Company when the opportunity to do so arises. Employees, officers and directors are prohibited, without the express written consent of the Board of Directors, from taking for themselves or using Company property, information or position for improper personal gain, and no employee may compete with the Company directly or indirectly.

VI. FOREIGN BUSINESS OPPORTUNITIES

In today's global marketplace, it is important to understand and appreciate the laws and regulations governing our interactions with other countries. All Company employees, agents, partners, and representatives are expected to abide by the laws of the United States as well as the laws of other countries in which the Company conducts business. Payments or offers to pay, either directly or indirectly, any foreign or domestic government official to induce that official to influence business to Company, would not only violate Company policy, but may also violate the United States '*Foreign Corrupt Practices Act'*. Sanctions against the Company for any such violations could be severe, and may involve fines and loss of export licenses. Likewise, payments to foreign political parties and candidates on behalf of the Company may also violate the *Foreign Corrupt Practices Act*.

VII. POLICY ADMINISTRATION

The Company's goal is to integrate this Policy into our daily business activities. As an employee of the Company, you have a responsibility to understand and comply with this Policy. Guidelines for compliance, include, but are not limited to, the following:

• All employees who become aware of any acts contrary to this Policy should give this information to his or her supervisor, the Human Resources department or the Company's in-house counsel. If for any reason you feel uncomfortable reporting such incidents or issues to your supervisor, Human Resources or legal, you may inform any member of Executive Management.

• The Company will investigate all reports made as set forth above. In any such investigation, the Company will respect the rights of all parties concerned and principles of fairness and dignity will be applied.

• If a violation of the expressed terms or spirit of this Policy is found, the Company will take appropriate disciplinary action. Such action could include immediate termination and filing of criminal charges. In addition, disciplinary action will be taken against any supervisor or other employee who retaliates, directly or indirectly, or encourages others to do so, against an employee who reports a violation of this Policy. All employees have the right to raise concerns or to report misconduct without fear of retribution.

• In the event you are uncertain about whether or not an action is permitted by this Policy, that issue should be raised with the employees' supervisor, the Human Resource Department or legal. The Company encourages inquiries and will make no negative implications because of them.

• In the event that an employee, including a member of management or a director, feels that a waiver from one or more of the standards set out in this Policy is appropriate in certain circumstances, that person must present a written request for a waiver to the Board of Directors. Only the Board of Directors has authority to waive any provisions of this Policy, if, in the Boards sole discretion, the waiver is in the best interests of the Company.

Note: This policy is subject to the Notice on the Company's Handbook.