

**A White Paper on:**  
**The Sarbanes-Oxley Act  
and Its Impact on IT**

**Prepared By:**  
**Mir F. Ali, Managing Partner**  
**AIMCORP-Automated Information Management**  
**Suite 663, 185-911 Yates Street**  
**Victoria, British Columbia, Canada V8V 4Y9**

**Tuesday, March 19, 2004**  
Modified on April 13, 2004

**A White Paper on:  
The Sarbanes-Oxley Act and Its Impact on IT**

---

This white paper is the product of the information available on the public domain, mainly on the Internet. The author has reviewed, analyzed, formulated, and supported the relevant information with the graphs to help understand the spirit of the ACT as well as the compliance mechanism.

**Mir F. Ali**

**TABLE OF CONTENTS**

1. Background	Page: 4
2. The Act	5
3. Cosponsors of the Act	7
4. Impact on Non-US Companies	7
5. Impact on IT	10
6. Conclusion	16
7. Update	17

**1. BACKGROUND:**

The year 2001 will also be remembered for the largest corporate bankruptcy in U.S. history. The collapse and bankruptcy of Enron Corporation, which had been the seventh-largest corporation in the United States, this year was a shocking and unexpected event but unfortunately it was far from an isolated case. It was in fact part of a pattern in which a number of major and highly-regarded public companies and their auditors relied upon convoluted and fraudulent accounting devices to inflate earnings.

<sup>1</sup>These practices took a terrible toll. Trillions of dollars in market value simply evaporated. Millions of individual investors watched helplessly as their savings diminished – and along with their savings, their plans and hopes for their retirement, or for their children’s education. Major pension funds were hard hit. Tens of thousands of men and women were thrown out of work. Understandably, investor confidence plummeted. With more than half of all American households invested in the securities markets, the entire country felt the impact.

The Wall Street Journal described it “The scope and scale of the corporate transgressions of the late 1990s now coming to light exceed anything the U.S. has witnessed since the years preceding the Great Depression.”

The Senate Banking Committee undertook to determine the depth and scope of the problems in the markets by conducting a series of ten hearings during the months of February and March in 2002. The hearings brought together preeminent regulators, scholars, practitioners and public interest representatives to discuss urgent accounting and investor protection issues and also to propose solutions. They found certain problems to be systemic and widespread, involving the executives and boards of too many public companies, accounting firms, stock analysts, regulators and others. They concluded that the problems could not be dealt with effectively by continuing accounting industry self-regulation, or within the existing statutory framework. They decided to create a statutory infrastructure that would strengthen the existing laws. They were convinced that it was an absolutely essential step toward restoring the integrity of the securities markets and the confidence of investors.

Senator Sarbanes led this initiative and drafted the legislation with the help of several major contributors including the members of the committee, notably Senators Dodd, Corzine, Enzi and Shelby, as well as numerous members off the Committee, including Senators Leahy, Hatch and Biden. Senator Sarbanes worked closely with chairman Oxley, in the conference to develop the final legislation and assure its final passage.

The Sarbanes-Oxley Act (SOA) was enacted on July 30, 2002 and signed into law by President George W. Bush. There are many elements to SOA, including sections that were intended to enhance and tighten financial disclosures, improve “whistle-blower” processes and the well-known requirement for the corporation’s financial statements to be certified by the CEO and CFO. Very importantly, SOA also creates and expands on existing criminal penalties for misrepresentations.

The legislation creates a strong independent oversight board to oversee the auditors of public companies and enables the board to set accounting standards, and investigate and discipline accountants. It addresses conflicts of interest, ensures auditor independence, strengthens corporate governance, by requiring corporate leaders to be personally responsible for the accuracy of their company’s financial reports, and establishes safeguards to protect against investment analysts’ conflicts.

---

<sup>1</sup> Remarks of Senator Paul S. Sarbanes at the Securities and Exchange Commission on Jul 30, 2003.

The Security and Exchange Commission (SEC) is the government agency charged with implementing most of the provisions of SOA. The SEC is an "independent agency," which means that it has aspects of all three branches of the federal government: executive, legislative and judicial powers. The SEC has civil (not criminal) enforcement powers against people who violate the securities laws and the rules; it has power to write rules pursuant to statute; and it acts like an appellate court in reviewing appeals from sanctions that the stock exchanges and the professional organization of brokers levy against their members.

The SOA required the SEC to make many rules within specific time limits. In the United States, the SEC is bound by law to give people subject to the rules fair notice of what rules the SEC plans to adopt and to have an opportunity to send comments on and objections to those rules. The SEC is required by law to take those comments into account and say why the SEC accepts or rejects those objections. The SEC is in the process of implementing the statute with diligence and skill. It has adhered to the timetable set out in the Act. It has taken public comment into account in writing numerous complex regulations. It has remained faithful both to the spirit as well as the letter of the statute.

Under Bill Donaldson, the Commission also moved decisively to assure strong leadership at the new Public Company Accounting Oversight Board (PCAOB). The PCAOB is central to the reform framework. Under Chairman Bill McDonough the PCAOB is up and running. The agency has the critical responsibility of overseeing the accounting firms. Given the leadership now in place at both the SEC and the PCAOB, it is expected that the Act is being implemented effectively.

## **2. THE ACT:**

The SOA promotes greater transparency and control in the accounting process and all registered companies (CEOs and CFOs) in America are obliged to submit formal declarations of the correctness of their accounting processes. Misinformation is punishable by fines of up to \$5 million and/or up to 20 years imprisonment.

The Act is divided into the following 11 categories:

<b>TITLE I—PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD:</b>	
<b>Sec. 101</b>	Establishment; administrative provisions.
<b>Sec. 102</b>	Registration with the Board.
<b>Sec. 103</b>	Auditing, quality control, and independence standards and rules.
<b>Sec. 104</b>	Inspections of registered public accounting firms.
<b>Sec. 105</b>	Investigations and disciplinary proceedings.
<b>Sec. 106</b>	Foreign public accounting firms.
<b>Sec. 107</b>	Commission oversight of the Board.
<b>Sec. 108</b>	Accounting standards.
<b>Sec. 109</b>	Funding.

<b>TITLE II—AUDITOR INDEPENDENCE:</b>	
<b>Sec. 201</b>	Services outside the scope of practice of auditors.
<b>Sec. 202</b>	Pre-approval requirements.
<b>Sec. 203</b>	Audit partner rotation.
<b>Sec. 204</b>	Auditor reports to audit committees.
<b>Sec. 205</b>	Conforming amendments.
<b>Sec. 206</b>	Conflicts of interest
<b>Sec. 207</b>	Study of mandatory rotation of registered public accounting firms.
<b>Sec. 208</b>	Commission authority.

<b>Sec. 209</b>	Considerations by appropriate State regulatory authorities.
-----------------	---

<b>TITLE III—CORPORATE RESPONSIBILITY:</b>	
<b>Sec. 301</b>	Public company audit committees.
<b>Sec. 302</b>	Corporate responsibility for financial reports.
<b>Sec. 303</b>	Improper influence on conduct of audits.
<b>Sec. 304</b>	Forfeiture of certain bonuses and profits.
<b>Sec. 305</b>	Officer and director bars and penalties.
<b>Sec. 306</b>	Insider trades during pension fund blackout periods.
<b>Sec. 307</b>	Rules of professional responsibility for attorneys.
<b>Sec. 308</b>	Fair funds for investors.

<b>TITLE IV—ENHANCED FINANCIAL DISCLOSURES:</b>	
<b>Sec. 401</b>	Disclosures in periodic reports.
<b>Sec. 402</b>	Enhanced conflict of interest provisions.
<b>Sec. 403</b>	Disclosures of transactions involving management and principal stockholders.
<b>Sec. 404</b>	Management assessment of internal controls.
<b>Sec. 405</b>	Exemption.
<b>Sec. 406</b>	Code of ethics for senior financial officers.
<b>Sec. 407</b>	Disclosure of audit committee financial expert.
<b>Sec. 408</b>	Enhanced review of periodic disclosures by issuers.
<b>Sec. 409</b>	Real time issuer disclosures.

<b>TITLE V—ANALYST CONFLICTS OF INTEREST:</b>	
<b>Sec. 501</b>	Treatment of securities analysts by registered securities associations and national securities exchanges.

<b>TITLE VI—COMMISSION RESOURCES AND AUTHORITY:</b>	
<b>Sec. 601</b>	Authorization of appropriations.
<b>Sec. 602</b>	Appearance and practice before the Commission.
<b>Sec. 603</b>	Federal court authority to impose penny stock bars.
<b>Sec. 604</b>	Qualifications of associated persons of brokers and dealers.

<b>TITLE VII—STUDIES AND REPORTS:</b>	
<b>Sec. 701</b>	GAO study and report regarding consolidation of public accounting firms.
<b>Sec. 702</b>	Commission study and report regarding credit rating agencies.
<b>Sec. 703</b>	Study and report on violators and violations
<b>Sec. 704</b>	Study of enforcement actions.
<b>Sec. 705</b>	Study of investment banks.

<b>TITLE VIII—CORPORATE AND CRIMINAL FRAUD ACCOUNTABILITY:</b>	
<b>Sec. 801</b>	Short title.
<b>Sec. 802</b>	Criminal penalties for altering documents.
<b>Sec. 803</b>	Debts non-dischargeable if incurred in violation of securities fraud laws.
<b>Sec. 804</b>	Statute of limitations for securities fraud.
<b>Sec. 805</b>	Review of Federal Sentencing Guidelines for obstruction of justice and extensive criminal fraud.

Sec. 806	Protection for employees of publicly traded companies who provide evidence of fraud.
Sec. 807	Criminal penalties for defrauding shareholders of publicly traded companies.

**TITLE IX—WHITE-COLLAR CRIME PENALTY ENHANCEMENTS:**

Sec. 901	Short title.
Sec. 902	Attempts and conspiracies to commit criminal fraud offenses.
Sec. 903	Criminal penalties for mail and wire fraud.
Sec. 904	Criminal penalties for violations of the Employee Retirement Income Security Act of 1974.
Sec. 905	Amendment to sentencing guidelines relating to certain white-collar offenses.
Sec. 906	Corporate responsibility for financial reports.

**TITLE X—CORPORATE TAX RETURNS:**

Sec. 1001	Sense of the Senate regarding the signing of corporate tax returns by Chief Executive officers.
-----------	---

**TITLE XI—CORPORATE FRAUD AND ACCOUNTABILITY:**

Sec. 1101	Short title.
Sec. 1102	Tampering with a record or otherwise impeding an official proceeding.
Sec. 1103	Temporary freeze authority for the Securities and Exchange Commission.
Sec. 1104	Amendment to the Federal Sentencing Guidelines.
Sec. 1105	Authority of the Commission to prohibit persons from serving as officers or directors.
Sec. 1106	Increased criminal penalties under Securities Exchange Act of 1934.
Sec. 1107	Retaliation against informants.

**3 COSPONSORS OF THE ACT:**

**Paul S. Sarbanes:**

Paul Spyros Sarbanes, Maryland's Democratic senior Senator, made Maryland history in November, 2000 by winning reelection to an unprecedented 5th term to the United States Senate, becoming the State's longest serving United States Senator.

Senator Sarbanes has been working for the people of Maryland for more than three decades, first as a member of the Maryland House of Delegates and then serving as a Congressman from the Third Congressional District for three terms. Since 1977, he has served with integrity and distinction in the United States Senate where he serves as the Ranking Member of the [Senate Banking, Housing and Urban Affairs Committee](#), and is a senior member of the [Foreign Relations, Budget and Joint Economic Committees](#).

**Michael G. Oxley:**

Congressman Oxley, Republican for Fourth Ohio District, is serving his eleventh full term in the House of Representatives and is Chairman of the new House Committee on Financial Services.

Congressman Oxley leads 37 Republicans, 32 Democrats, and 1 Independent on the Committee, which oversees Wall Street, banks, and the insurance industry. In addition to financial matters, Oxley has a long involvement with trade, telecommunications, and energy issues. A firm believer

in market competition, Oxley draws on his business and financial expertise to advocate policies promoting personal savings, jobs, and economic growth.

#### **4 IMPACT ON NON-US COMPANES:**

While the SEC is engaged in converting the elements of the Act into rules and implementing them in pursuing their primary mission to protect investors, they have to be mindful of the special considerations and needs of their non-U.S. issuers. For many years, U.S. investors have been seeking opportunities to invest in the securities of non-U.S. issuers, including German issuers. The SEC has long recognized the importance of the globalization of the securities markets both for investors looking for increased diversification and international entities looking for capital-raising opportunities in different, and sometimes larger, markets. In addition, allowing non-U.S. issuers access to the U.S. securities markets gives these non-U.S. issuers "acquisition currency" to make acquisitions in the U.S.

<sup>2</sup>Over 1,300 non-U.S. corporations from 59 countries file reports with the SEC, as compared with approximately 400 issuers from less than 30 countries in 1990. Most of the non-U.S. issuers are from **Canada**. The second largest numbers are from the U.K. Currently, approximately 30 German corporations report to the SEC.

The SOA generally makes no distinction between U.S. and non-U.S. issuers. The Act does *not* provide any specific authority to exempt non-U.S. issuers from its reach. The Act leaves it to the SEC to determine where and how to apply the Act's provisions to foreign companies. The SEC is well aware that new U.S. requirements may come into conflict with requirements on non-U.S. investors-issuers.

The SEC has released and proposed the following rules and their implications to non-U.S. issuers:

- **Public Company Accounting Oversight Board (PCAOB):**

The Act directed the SEC to create a new Public Company Accounting Oversight Board to oversee the accounting profession and public company audits. It was created because of deep failings in the U.S. accounting profession's ability to regulate itself. The Oversight Board is a non-governmental, nonprofit corporation and must consist of five full-time independent members.

Of understandable concern to the public is the fact that the Act requires foreign public accounting firms that audit SEC-registered issuers, including non-U.S. issuers, to register with the Oversight Board and be subject to its oversight. Ultimately, the decision must balance the fundamental regulatory objectives of SOA with the role as one of many regulators in the community of nations.

- **Audit Committees:**

One of the most significant aspects of SOA is expanding the role and responsibilities of audit committees. The SOA requires the audit committee to be responsible for the outside auditor relationship, including the responsibility for the appointment, compensation, and oversight of a company's outside auditor. And, the Act requires that members of the audit committee be "independent" from company management.

The idea of seeking "independence" of board members is not a new concept in the U.S. As early as 1972, the SEC recommended audit committees of "outside directors". In 1976 a

---

<sup>2</sup> Speech by SEC Commissioner, The Sarbanes-Oxley Act of 2002: Goals, Content, and Status of Implementation by Commissioner Paul S. Atkins.

Congressional committee reported a need for directors that are "detached" from "management and from any other conflict of interest". More recently, a SEC-led committee on improving the effectiveness of audit committees recommended that all audit committee members be independent from corporate management.

Many non-U.S. issuers already have independent audit committees as part of their corporate governance structure and the global trend appears to be toward setting up such audit committees. There is almost universal support for some form of independent check on company management by a disinterested board. Indeed, the German corporate governance code makes recommendations regarding obtaining more independence of the supervisory board members from company management. In the U.K., the value of independent directors is emphasized in the recommendations of Derek Higgs regarding corporate governance, building on the earlier work of the Cadbury Commission.

▪ **Financial Experts:**

The SOA also directs the SEC to adopt rules requiring the disclosure of whether a company has a "financial expert" on its audit committee and to define a "financial expert". The SEC has recently released rules in response to this directive. Indeed, studies show that companies that have board members with significant financial knowledge need to restate the financial statements less than companies with less-experienced board members.

In the final rule, every issuer, including a non-U.S. issuer, will need to disclose whether it has a financial expert on its board and whether the financial expert is independent from management. However, non-U.S. issuers will not be required to make this disclosure until the final rules regarding audit committees are in place. The SEC has decided to delay the disclosure requirement because they recognize that the non-U.S. issuers have never been subject to independent audit committee disclosure. The SEC acknowledges that imposing this financial expert disclosure requirement on non-U.S. issuers in such a short timeframe would be unfair. The SEC trusts that non-U.S. issuers will be more comfortable with this disclosure requirement by the time the overall audit committee rules are effective.

▪ **Attorneys:**

The SEC was directed by the SOA to adopt final rules regarding "minimum standards of professional conduct" for attorneys. The SEC acknowledges that it is in un-chartered waters with these new rules. They have been referred to as the first significant effort by Congress to mandate the U.S. federal regulation of lawyers.

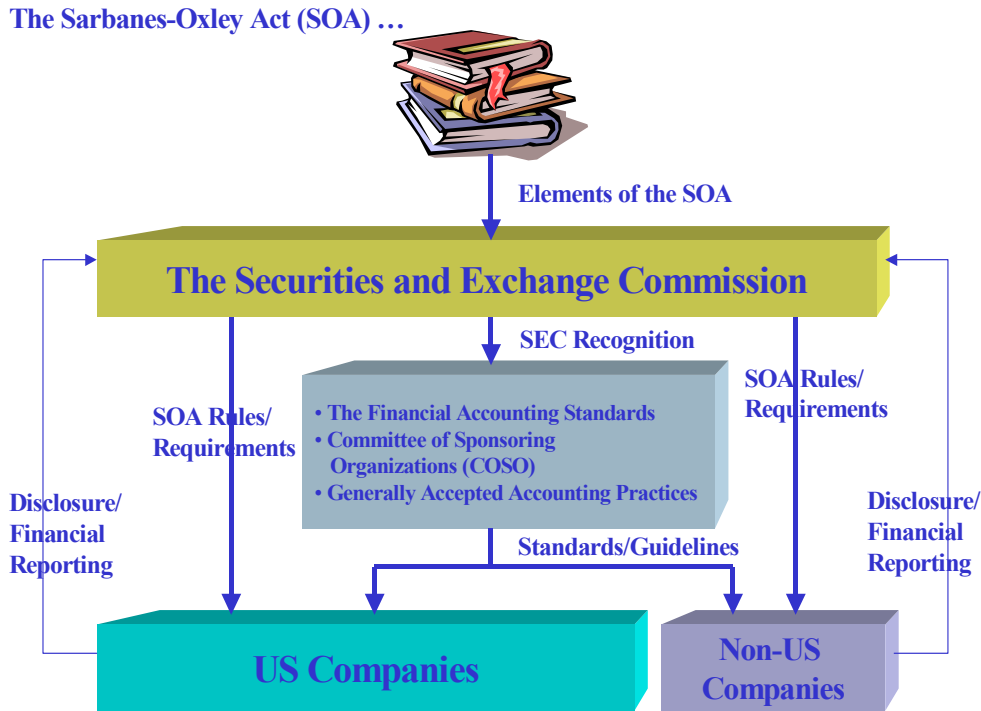
The SEC proposed rules in December (2002) and received approximately 170 comment letters regarding the proposal, including over 40 from foreign parties. The proposed rule was controversial in many ways. It took an expansive view of who could be found to be "appearing and practicing" before the SEC. It reached attorneys licensed in foreign jurisdictions, whether or not they were also admitted in the United States. And it raised issues of jurisdiction and enforceability.

The SEC's recently released final rule is less controversial. It has been significantly modified because of the many thoughtful comments and suggestions that the SEC received. The SEC has exempted from the rule certain foreign attorneys. The SEC calls them "Non-Appearing Foreign Attorneys". If an attorney falls within this definition, that attorney is not subject to the rule's requirements. In order to satisfy the Non-Appearing Foreign Attorney test, the individual must:

- Be admitted to practice outside the U.S.;

- Does not give advice or hold himself out as practicing U.S. federal or state securities laws; and
- Conducts activities that would constitute appearing and practicing before the SEC only incidentally to, and in the ordinary course of, the practice of law in a jurisdiction outside the U.S.; or appears and practices before the SEC only in consultation with a U.S. attorney. The SEC has also specifically stated that even if an attorney is subject to the new rule, this attorney shall not be required to comply if the rule conflicts with local law.

The following graph is designed to illustrate the interfaces between the US Companies and Non-US Companies for ensuring the compliance of SOA:



AIMCORP – Automated Information Management Corporation

Figure 1

**5 IMPACT ON IT:**

It is imperative to understand that the SOA is not about technology. The focus of this Act is on improving transparency and accountabilities in business processes and corporate accounting to restore confidence in public markets. It regulates processes and business practices, not technology. In the modern enterprise, however, technology often defines and executes business processes or parts of business processes. The technology and business process regulated by the SOA are so entwined that it's impossible to separate them.

According to analyst John Hagerty of AMR Research, which released a survey recently on the impact of the law, *\$2.5 billion is just the tip of the iceberg*. Eight-five percent of 60 companies that responded to the AMR Research survey said the SOA will require changes to their IT and application infrastructure.

Additionally, two provisions in the law that have yet to take effect may fuel new IT projects, said Hagerty. Section 404, which public companies must begin to comply with by the end of the year, pertains to the certification of financial reporting and controls. Section 409, which Hagerty said doesn't have a clear compliance deadline, calls for companies to report material financial events as they occur, rather than at the end of their financial quarter.

As companies update their business systems to help them comply with the law, they could "kick-start" corporate spending on IT the same way the much-feared Y2K bug spurred companies to install or update software programs in time for the year 2000 date change, AMR said. "It's reminiscent of the enterprise resource planning software craze Y2K kicked off in the 1990s," the study stated. Rather than patch aging business systems, many companies used the Y2K scare as a reason to install new applications from companies such as SAP, PeopleSoft and Oracle. Fueled partly by the Y2K boom, those software companies reaped big profits and reported double-digit growth during the late 1990s.

To be sure, Sarbanes-Oxley won't have as big an impact on the computer industry as the millennium change did, Hagerty said. And IT consultants will likely soak up much of the IT investment, he added. Still, compliance may spark some new activity in corporate IT departments, which have been idling for more than two years in response to a weak economy.

Bringing the systems into compliance with a new financial reporting law may be the biggest information-technology expenditure this decade. Some say implementing compliance with the SOA is a bigger project than Y2K bug fixes. "That might seem extreme," says Kraig Haberer, director of financial product marketing at SAP. "But Y2K was a single task —this is a recurring one. "We've seen clients invest tens of thousands of hours to achieve minimal Sarbanes-Oxley compliance," says Gregory Derderian, managing director of the World-Class Finance practice at consultancy BearingPoint.

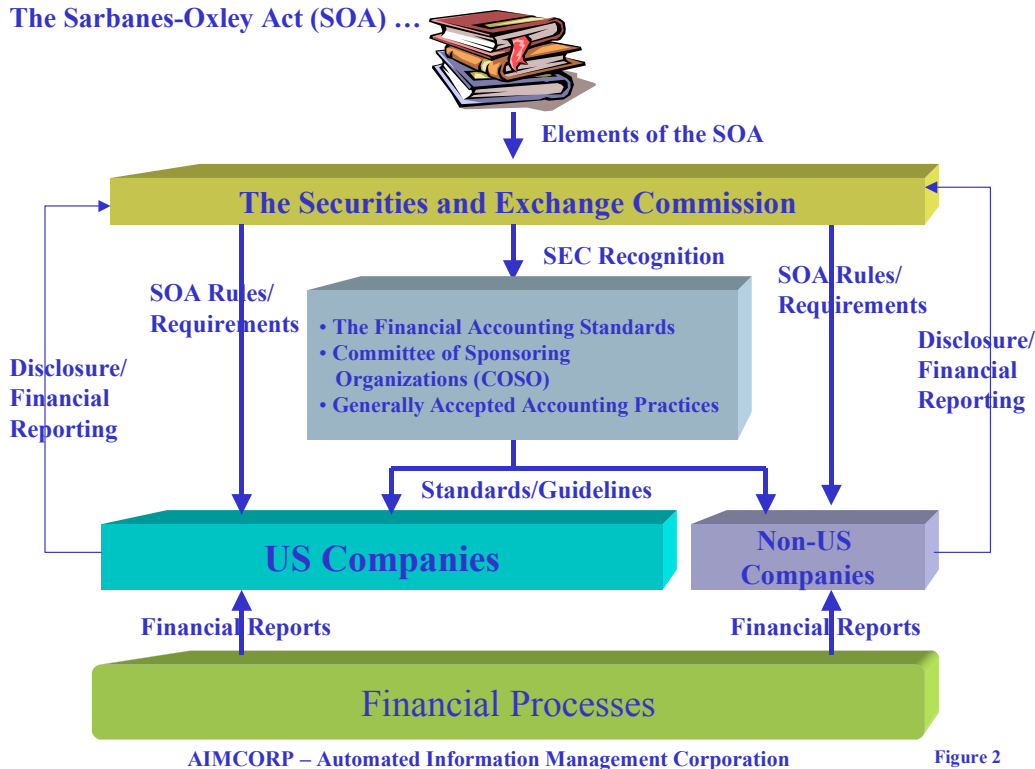
The Big Four auditing firms, on which most large companies are relying to help them through the compliance process, are recommending the use of the Committee of sponsoring Organizations of the Treadway Commission (COSO) Risk management Framework. This framework is designed to instill "risk and control consciousness," and is a model for discussing and comparing risk management and internal controls. The COSO Framework contains specific IT-related advice.

<sup>3</sup>COSO is a voluntary, private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal control and corporate governance. It was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector organization often referred to as the Treadway Commission. The sponsoring organizations include the AICPA, American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Management Accountants (IMA).

The graph presented on the next page illustrates the connectivity of the financial processes:

---

<sup>3</sup> IT Control Objectives For Sarbanes-Oxley By IT Governance Institute



COSO identifies five essential components of effective internal control. The following is a description of each component and its relationship to IT:

**1. Control Environment:**

Control environment creates the foundation for effective internal control, establishes the “tone at the top,” and represents the apex of the corporate governance structure. The issues raised in the control environment component apply throughout an organization.

The control environment primarily addresses the company level. However, IT frequently has characteristics that may require additional emphasis on business alignment, roles and responsibilities, policies and procedures, and technical competence. The following list describes some considerations related to the control environment and IT:

- IT is often mistakenly regarded as a separate organization of the business and thus a separate control environment;
- IT is complex, not only with regard to its technical components but also as to how those components integrate into the company’s overall system of internal control;
- IT can introduce additional or increased risks that require new or enhanced control activities to mitigate successfully;
- IT requires specialized skills that may be in short supply;
- IT may require reliance on third parties where significant processes or IT components are outsourced; and
- The ownership of IT controls may be unclear.

## **2. Risk Assessment:**

Risk assessment involves the identification and analysis by management of relevant risks to achieve predetermined objectives, which form the basis for determining control activities. It is likely that internal control risks could be more pervasive in the IT organization than in other areas of the company.

Risk assessment may occur at the company level (for the overall organization) or at the activity level (for a specific process or business unit).

At the company level, the following may be expected:

- An IT planning subcommittee of the company's overall Sarbanes-Oxley steering committee. Its responsibilities may include the following:
  - Oversight of the development of the IT internal control strategic plan, its effective and timely execution/implementation, and its integration with the overall Sarbanes-Oxley compliance plan; and
  - Assessment of IT risks, e.g., data security, availability and performance analysis.

At the activity level, the following may be expected:

- Formal risk assessments built throughout the systems development methodology;
- Risk assessments built into the infrastructure operation and change process; and
- Risk assessments built into the program change process.

## **3. Control Activities**

Control activities are the policies, procedures and practices that are put into place to ensure that business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified. Control activities primarily address the activity level. Without reliable information systems and effective IT control activities, public companies would not be able to generate accurate financial reports. COSO recognizes this relationship and identifies two broad groupings of information system control activities:

- **General Controls:**

General controls, which are designed to ensure that the financial information generated from a company's application systems can be relied upon, include the following types:

  - **Data center operation controls**—Controls such as job setup and scheduling, operator actions, backup and recovery procedures, and contingency or disaster recovery planning;
  - **System software controls**—Controls over the effective acquisition, implementation and maintenance of system software, database management, telecommunications software, security software and utilities;
  - **Access security controls**—Controls that prevent inappropriate and unauthorized use of the system;
  - **Application system development and maintenance controls**—Controls over the development methodology, which include system design and

implementation, outlining specific phases, documentation requirements, approvals, and checkpoints to control the development or maintenance of the project

○ **Application Controls:**

Application controls are embedded within software programs to prevent or detect unauthorized transactions. When combined with other controls, as necessary, application controls ensure the completeness, accuracy, authorization and validity of processing transactions. Some examples of application controls include:

- **Balancing control activities**—These controls detect data entry errors by reconciling amounts captured either manually or automatically to a control total. For example, a company automatically balances the total number of transactions processed and passed from its online order entry system to the number of transactions received in its billing system;
- **Check digits**—Calculations to validate data. A company's part numbers contain a check digit to detect and correct inaccurate ordering from its suppliers. Universal product codes include a check digit to verify the product and the vendor;
- **Predefined data listings**—Provide the user with predefined lists of acceptable data. For example, a company's intranet site might include dropdown lists of products available for purchase;
- **Data reasonableness tests**—Compare data captured to a present or learned pattern of reasonableness. For example, an order to a supplier by a home renovation retail store for an unusually large number of board feet of lumber may trigger a review; and
- **Logic tests**—Include the use of range limits or value/alphanumeric tests. For example, credit card numbers have a predefined format.

General controls are needed to support the functioning of application controls, and both are needed to ensure accurate information processing and the integrity of the resulting information used to manage, govern and report on the organization. As application controls increasingly replace manual controls, general controls are becoming more important.

#### **4. Information and Communication**

COSO states that information is needed at all levels of an organization to run the business and achieve the entity's control objectives. However, the identification, management and communication of relevant information represent an ever-increasing challenge to the IT department. The determination of which information is required to achieve control objectives, and the communication of this information in a form and time frame that allows people to carry out their duties, supports the other four components of the COSO framework.

The IT organization processes most financial reporting information. However, its scope is usually much broader. For example, the IT department may also assist in implementing mechanisms to identify and communicate significant events, such as e-mail systems or executive decision support systems.

COSO also notes that the quality of information includes ascertaining whether the information is:

- Appropriate—Is it the right information?
- Timely—Is it available when required and reported in the right period of time?
- Current—Is it the latest available?
- Accurate—Are the data correct?
- Accessible—Can authorized individuals gain access to it as necessary?

At the company level, the following may be expected:

- Development and communication of corporate policies;
- Development and communication of reporting requirements, including deadlines, reconciliation, and the format and content of monthly, quarterly and annual management reports; and
- Consolidation and communication of financial information.

At the activity level, the following may be expected:

- Development and communication of standards to achieve corporate policy objectives;
- Identification and timely communication of information to assist in achieving business objectives; and
- Identification and timely reporting of security violations.

## **5. Monitoring:**

Monitoring, which covers the oversight of internal control by management through continuous and point-in-time assessment processes, is becoming increasingly important to IT management. There are two types of monitoring activities: continuous monitoring and separate evaluations.

IT performance and effectiveness are increasingly monitored using performance measures that indicate if an underlying control is operating effectively. Consider the following examples:

- **Defect identification and management**—Establishing metrics and analyzing the trends of actual results against metrics can provide a basis for understanding the underlying reasons for processing failures. Correcting these causes can improve system accuracy, completeness of processing and system availability; and
- **Security monitoring**—Building an effective IT security infrastructure reduces the risk of unauthorized access. Improving security can reduce the risk of processing unauthorized transactions and generating inaccurate reports, and can ensure a reduction of the availability of key systems if applications and IT infrastructure components have been compromised.

An IT organization also has many different types of separate evaluations, including:

- Internal audits;
- External audits;
- Regulatory examinations;
- Attack and penetration studies;
- Independent performance and capacity analyses;
- IT effectiveness reviews;
- Control self-assessments;
- Independent security reviews; and

- Project implementation reviews

At the company level, the following may be expected:

- Centralized continuous monitoring of computer operations;
- Centralized monitoring of security; and
- IT internal audit reviews (While the audit may occur at the activity level, the reporting of audit results to the audit committee will be at the company level.)

At the activity level, the following may be expected:

- Defect identification and management;
- Local monitoring of computer operations or security; and
- Supervision of local IT personnel.

## **6. CONCLUSION:**

Several public estimates indicate that the total independent accounting fees, including tax audits, on the expanded disclosure forms required by the SOA have climbed 30 to 35 percent in 2003 over 2002. The cost of legal counsel/director/officer as well as insurance premium (which have exploded by at least 300 percent during the past two years) must be added to the total. Accordingly, the compliance is going to be a very expensive undertaking for the companies.

The reality is that the SOA is turning out to be an additional financial burden for the companies that are already suffering from fiscal constraints and searching for ways to minimize their operational as well as regulatory overheads. Perhaps the best way to help these companies is not only to assist them with compliance of this Act but also to show them how to use technology as a strategic tool, leveraging technology to reduce the resource burden of compliance.

**7. UPDATE:**

The first round of a financial-reporting auditing standard was made public last week, a step toward providing guidelines for companies struggling to implement systems compliant with the SOA.

Because of delays in developing the standard, the SEC recently pushed back to November 15, 2004, the deadline for compliance with section 404 of the SOA, which requires management and auditors to certify that a company's financial controls are in order. The extension to the deadline, which was June 15, 2004, gives the Public Company Accounting Oversight Board, a quasi-government body of accounting pros, more time to work on the auditing standard it adopted last week. After a six-week period for public comment, the standard will go to the SEC for final approval.