SOX Section 404 – US Experience In Corporate Governance

Pradeep Godbole

The author is a Principal Consultant at I-Flex Consulting. He can be reached at pradeep.godbole@iflexsolutions.com

Sarbanes Oxley Act, 2002 (SOX), enacted as a result of the recent corporate failures in the US, has changed corporate governance landscape in US - particularly, Section 404 of the Act — Management Assessment of Internal Controls. Section 404 casts onerous responsibilities on CEOs and CFOs, as well as external auditors of publicly listed companies. This article examines the provisions of Section 404, the challenges and learnings from US experience and finally, the comparison of SOX vis a vis provisions in India.

Backdrop of SOX — Corporate and Financial Accounting Scandals

Corporate America has witnessed an unprecedented string of corporate and financial accounting scandals in recent times—Enron, WorldCom, Global Crossing, to name a few. Even top-rung companies such as Xerox had to make major restatements to their financial statements. These failures occurred despite the existence of corporate governance standards, as well as a well-developed regulatory and financial reporting framework in the USA.

Sarbanes-Oxley Act (SOX), enacted in the year 2002, was a drastic measure to improve corporate governance and regain investor trust and confidence. Of the 300 sections in the Act, Section 404 has had the most profound effect and can easily be categorised as one of the most power-packed legislations ever.

Section 404—Focus on Internal Controls

While there are many reasons attributable for the aforesaid corporate failures, the most prominent among them is the failure of organisations to ensure accuracy, reliability and transparency of their financial reports. Naturally, a significant thrust of SOX is on strengthening internal controls over financial reporting.

Section 404 requires CEOs/CFOs of such organisations to provide an 'Internal Control Report' on an annual basis, asserting that they are responsible for the following:

- Establishing and maintaining internal control structures and financial reporting procedures.
- Using a framework for the assessment of internal controls over financial reporting.
- Evaluating the existence and effectiveness of internal control structures and financial reporting procedures at the end of the financial year.

Any significant deficiency or material weaknesses in the operation of internal controls require disclosure to the Audit Committee and the External Auditor.

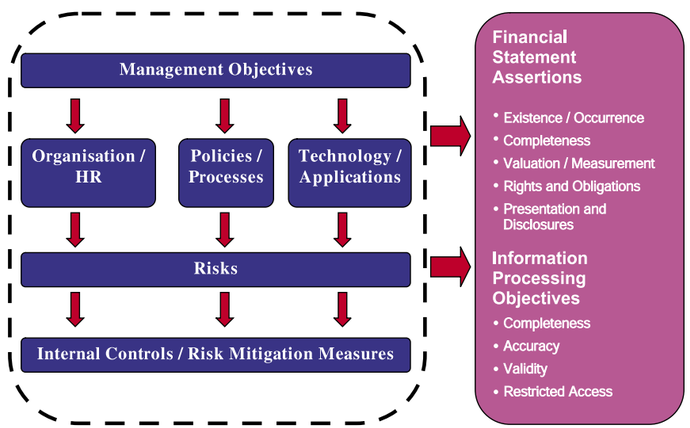
The External Auditors, who report on the financial statements, have to attest and report on the management assessment of internal controls. The Auditor will have to consider the significant deficiencies and material weaknesses while giving their opinion and have to ensure that the Management has sufficient basis for its assessment of internal controls over financial reporting. Thus, the Act casts an additional responsibility of attesting and reporting on the management assessment of internal controls for the External Auditor.

Section 404 of SOX applies to all publicly listed companies filing annual reports under Section 13(a) and 15(d) of the Securities Exchange Act, 1934, except investment companies and issuers of asset-backed securities. Subsidiaries and divisions of companies of such companies (even located outside US) and foreign private issuers (irrespective of country of origin) fall under the purview of the Act. Even outsourced activities including cross border outsourcing is within Section 404 purview. Thus, SOX 404 net is cast far and wide.

The deadline for compliance for organisations with public equity of more than USD 75 Million was November 15, 2004, while others are expected to adhere to the cut-off date of July 16, 2006. Another point to note here is - while the External Auditor certification is on an annual basis, the Management has to report on a quarterly basis. Thus, this is not a one time effort but an on-going commitment.

While Section 404 looks innocuous on plain reading, it is backed by cutting-edge penalty provisions. Any inadvertent wrong certification attracts a penalty of USD 1 Million or an imprisonment of 10 years, or both, while the penalties for deliberate acts attract higher penalty at USD 5 Million or an imprisonment of 20 years, or both. These penalties enforce high visibility to the internal controls framework across the organisation.

Organisational perspective of Section 404



The intricate relationships between financial statements, processes and internal controls are portrayed in the figure above. A company's senior management team sets the objectives, which can be categorised into financial goals such as revenue, profit, market standing, market share and non-financial objectives such as innovation, consumer satisfaction, and contribution to the society or country's development, corporate citizenship. These goals are achieved through:

- People: Comprising human resources, organisational and HR policies and procedures, recruitment, training, compensation, ethics and code of conduct, amongst others.
- Processes: Business processes and procedures, authorisation matrices, segregation of duties and responsibilities, asset safeguarding and so on.
- Technology: Technology infrastructure and applications used in business processes.

There is a risk angle attached to all of the above—for instance, true and fair view can be distorted from simple error—wrong input of transaction or duplicate transaction processing to error from complex situations—valuation of exotic derivative instruments or estimates/judgments for non-performing assets. Internal controls under SOX purview includes:

- Entity level controls: Control environment and management philosophy, organisation structure, roles and responsibilities of various committees (management committee, audit committee, disclosure committee, compensation committee), HR policies and procedures, ethics and code of conduct, anti-fraud programs, whistle blower provisions, senior management oversight mechanisms including Internal Audit
- Business and Process Controls: Control over operating activities like policies and procedures, organisation structure, maker-checker, authorisation, segregation of duties, asset safeguarding and also monitoring controls like reconciliation, periodic reporting and reviews.
- IT Controls: IT controls include application controls such as those existing in software applications used as well as general IT controls such as, technology infrastructure, software development, con-

figuration management, change management, network and computer access controls, and data center management.

The culmination of operations, transaction processing and reporting are financial statements, which comprise the management's financial statement assertions or information-processing objectives, which are explained in greater depth in the table 01.

The financial statement assertions and information-processing objectives read more or less similar; however, the critical difference between them is that information-processing objectives mainly rely on application controls for transaction-processing, while financial statement assertions are directed towards fair financial reporting.

Sound Internal Control Framework

As mentioned above, the internal control framework is critical to ensuring accuracy, reliability and transparency of financial reporting and is at the heart of SOX regulation. While SOX has given organisations the freedom to choose the most suitable framework, the framework prescribed by COSO (The Committee of Sponsoring Organisations) has emerged as the most popular framework so far.

The Committee of Sponsoring Organisation (COSO), also known as the Treadway Commission, is a voluntary private sector organisation established in 1985. The sponsoring organisations of COSO are - AICPA (American Institute of Certified Public Accountants); AAA (American Accounting Association); FEI (Financial Executives International); IIA (Institute of Internal Auditors); IMA (Institute of Management Accountants). In 1992, the committee issued a landmark report on internal controls (Internal Control - Integrated Framework), which is often referred to as 'COSO Framework'.

COSO defines internal controls as a process created by an entity's board of directors, management and other personnel, and designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Operations - ensuring effectiveness and efficiency of operations
- Financial reporting - focusing on accuracy, reliability and timeliness of financial reporting
- Compliance - with applicable laws and regulations

There are five components of the Internal Control Framework as under in Table 02

In 2004, COSO has released Enterprise Risk Management framework (ERM) which extends 1992 framework and this may become a standard of the future.

As mentioned above, internal controls under SOX purview, not only include business and process controls but also IT controls. CoBIT provides an internal control framework more relevant from an IT controls perspective. CoBIT (Control Objectives for Information and Related Technology) standards were developed by the IT Governance Institute of Information Systems Audit and Control Association (ISACA) in 1992.

Table 01

Financial Statement Assertions	Information-Processing Objectives
▪ Existence / Occurrence – All transactions are recorded in the correct period, with no duplications	▪ Completeness – All transactions are recorded and there are no duplications.
▪ Completeness – All transactions are recorded and reported and that there are no omissions	▪ Accuracy – The amounts, time period and accounts in which the transactions are recorded are accurate.
▪ Valuation / Measurement – The transactions are recorded at correct amount	▪ Validity – Ensure proper authorisation of transactions, with no fictitious transactions.
▪ Rights and Obligation – The organisation has legal right to the assets and only genuine obligations are recorded as liabilities.	▪ Restricted Access – The physical, application and logical access are restricted
▪ Presentation and Disclosure – The financial statement item is correctly classified and disclosed.	

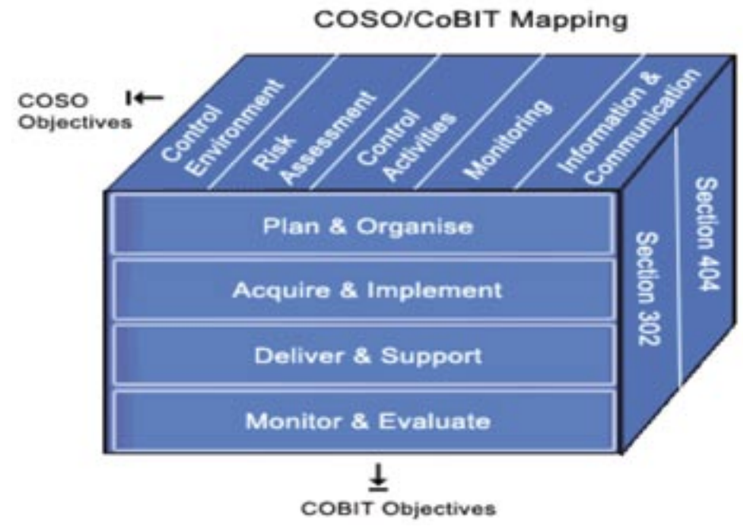
Table 02

Control Environment	Management commitment and attitude to the implementation and maintenance of an effective internal control structure. It provides structure and fundamental discipline
Risk Assessment	Identification, analysis, assessment and prioritisation of risks. This is a major component of effective Internal Control structure
Control Activities	Policies and procedures that ensure ▪ Mitigation of risks ▪ Prevention, detection and correction of irregularities ▪ Safeguarding of assets from unauthorised use or disposal ▪ Accuracy and reliability of financial reporting
Information and Communication	Dissemination of control responsibilities to employees in a form and within a time frame that allows them to carry out their duties
Monitoring	Review the effectiveness of the internal controls on an ongoing basis or through separate reviews and evaluations

CoBIT has 34 High-Level Control Objectives and 318 Detailed Control Objectives classified into four major domains, which are:

- Plan and Organise
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

CoBIT objectives are nothing but the best practices for management of IT processes by defining manageable and logical structure and bridging the gaps among business risks, technology issues, control needs and performance measurement. CoBIT objectives can be mapped to the COSO internal framework and can be used as a reference point for IT-related controls.



How SOX 404 implementations were done

Table 03

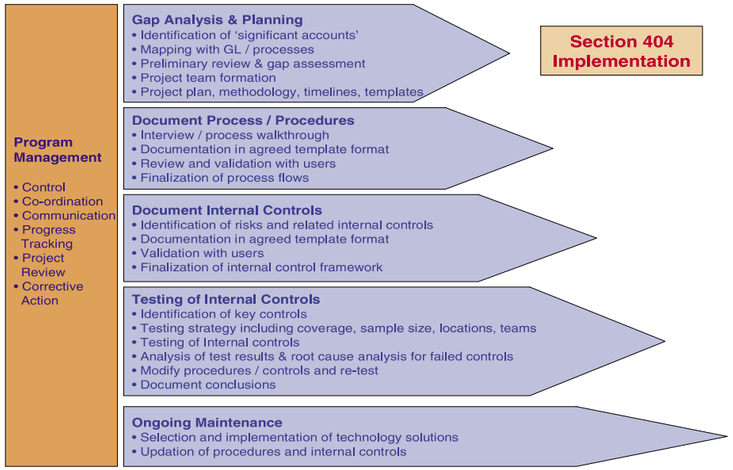
The typical SOX Section 404 compliance by and large involved the key phases described above. But this is easier said than done. Let us examine some of the key challenges and issues encountered during this process and also critical success factors, the learnings and trends emerging out of US experience. The learning process is still ongoing and will mature as organisations get experienced in the implementations.

Implementation challenges

- High cost and effort

The first and foremost challenge has been the enormous amounts of money, efforts and resources the organisations had to spend on Section 404 compliance. The spending and effort estimates in various surveys have been quite astounding.

Financial Executives International (FEI) surveyed costs estimates of 217 public companies with average revenues of $5 billion. The average total costs for Year 1 compliance was $4.36 million ($1.34 million for internal costs, $1.72 million for external costs and $1.30 million for auditor fees). This was 39 percent higher than $3.14 million as per FEI's earlier July 2004 cost survey. The increase stems largely from a 66 percent leap in external costs for consulting, software and other vendors and a 58 percent increase in the fees charged by external auditors.



Ernst and Young survey in 2004 estimates average hours expected to be spent in the implementation based on the size of company as under –

Less than USD 1 Billion	8,000 Hours
USD 1 - USD 5 Billion	14,000 Hours
USD 5 - USD 20 Billion	25,000 Hours
Greater than USD 20 Billion	80,000 Hours

- Compliance with multiple regulations and evolving regulations

Organisations have to comply with multiple regulations today –- SOX, Basel II, Patriot Act and Anti-Money Laundering, International Financial Reporting Standards and so on. Each of these is a major compliance initiative in itself and the organisations had to keep the cost and time factors under check while simultaneously ensuring quality.

The progressive organisations attempted to integrate multiple compliance initiatives. Some of the organisations integrated their already existing Risk and Controls Self Assessment frameworks with the SOX initiative while in other cases, the organisations are exploring ways to integrate Basel II operational risk initiative with SOX risk and control documentation. The next step in this journey will be to integrate SOX initiative with larger Enterprise wide Risk Management framework.

One of the other significant challenge in SOX implementation was - some of SOX guidance was available only after the organisations were well under way for SOX implementations. The participants were learning, understanding, analysing and applying the provisions on real time basis. The organisations had to be nimble and swift to address the impact of evolving regulations although it resulted in changing or re-working procedures and end up in wasteful efforts in some cases.

- Wide coverage

SOX is applicable to not only the parent company but also to its subsidiaries, and divisions. Since most large organisations have multiple businesses, departments, and locations, determination of the coverage – location, amounts, accounts was decisive. The organisations had to critically examine not only quantitative factors like dollar size but also qualitative factors like complexity and importance of the activity. The organisations had to also consider the impact and complexity of outsourced operations especially cross-border outsourcing. With wide coverage, the successful organisations had to effectively manage the 5Cs - control, co-ordination, communication, consistency, and coverage in all its activities.

- Project management

SOX initiative is not limited to just finance and accounting functions but encompasses the entire organisation. For mation of a project team with the right blend of experience, knowledge and skills was highly critical.

The projects were driven by an Executive Sponsor, typically CEO or CFO or the highest functionary in the organisation, to ensure that the required importance, attention, and patronage was given to this initiative. The project team in itself had to include representatives across locations and various functions such as business, operations, finance, internal audit, IT and risk management. The Project Manager had to play a pivotal role in success of the project. The project manager had to be an able manager, leader, communicator, with a sound knowledge of internal controls, business and IT.

With multiple compliance initiatives and the accompanying wide coverage, managing, tracking and monitoring the project was vital. Organisations had to put in a mechanism to constantly track the progress of multiple compliance activities and take corrective action thereon. The Project Office had to maintain continuous control, co-ordination and communication across the organisation to ensure that the project moved towards the final goal in a systematic and timely manner.

- Implementation approach and methodology

Determining the implementation approach and methodology under evolving regulations also proved to be a challenge and required consideration of various factors - type of organisation, identification of significant accounts, preliminary risk analysis of processes, number of processes to be covered, geographical locations to be covered, gap analysis of existing documentation, standards and depth of documentation, embedding IT controls in the documentation, effect of ongoing IT initiatives, testing strategy, timelines and resource plans, and so on. Involvement and inputs of the external auditor was also found to be beneficial throughout the project.

- IT Systems and Controls

IT is extensively used in transaction processing and financial reporting. However, most of the organisations lacked formal, adequate, consistent quality documentation of IT processes and controls and it was one of the weakest areas and cause of concern for many organisations. In many cases, IT managers were not involved in the implementation process upfront and resulted in last minute scramble.

IT also posed a unique problem - IT managers don't process information but they were accountable for the quality and integrity of information. SOX implementation highlighted glaring weaknesses in IT security and access controls. Most organisations had disparate IT systems involving system interfaces, data hand offs, file transfers which had data sync up and integrity issues. Another issue the institutions are still grappling with is the controls over the rampant use of Excel sheets – all these factors have magnified the risk dimensions.

- Testing

69 per cent of respondents in a PriceWaterhouseCoppers survey identified testing as a major challenge. A variety of factors had to be considered such as type of controls, identification of key controls for testing, scope and coverage of locations/businesses, types of testing, sample sizes and timing of the testing, independence and experience of testing resources, documentation of testing, evaluation of exceptions, remediation of failed controls and re-testing. The identification of key controls, the evaluation of effectiveness and existence of such controls and reporting significant deficiencies and material weaknesses were the critical steps in the chain. Many reputed organisations have reported significant deficiencies and material weaknesses in the operations of internal controls.

- Ongoing review and maintenance

SOX implementation is not a one-time exercise but an ongoing review of processes and internal controls. Internal procedures and controls are of a dynamic nature and can undergo changes often for e.g. introduction of new products, new lines of businesses, changes in organisation structure will require updates of existing documentation and controls. The organisations will have to establish an infrastructure for ongoing maintenance. Apart from integration with existing internal audit activities, some organisations are actively looking to 'outsource' the ongoing activities.

- Technology solutions for regulatory compliance

Since SOX is an ongoing exercise, technology will play a significant role in compliance. Many of the organisations have done their documentation in Microsoft tools but are looking at technology options for ongoing maintenance. Currently, there is no single solution for SOX compliance and the multiple regulatory compliance initiatives, but versatility, scalability and flexibility are the vital factors that need to be considered while implementing an IT solution. Further, the solution also has to integrate with existing systems, accommodate multiple compliance requirements, incorporate workflows, audit trails, information security, real-time processing, training and customisation needs. The progressive organisations will have to decide either on off the shelf product or customised development using compliance platform based framework/approach.

Learnings from US experience—is the cost and effort worth??

Significantly high – 94 per cent of companies in FEI survey believe that the costs of Section 404 compliance far exceed the benefits. Such exorbitant cost, effort and resource requirements forced many European companies to take a drastic step to de-list from US stock exchanges. However, delisting exit route is also time consuming and complicated - the number of US shareholders has to be less than 300. Also, the cost of delisting from one of vibrant financial markets has its own disadvantages.

So a question arises whether the enormous amount of cost and effort is worth and whether there is any significant difference vis a vis a situation before. The advocates of Section 404 strongly point out the benefits -

- First and foremost, the Act established clear accountabilities for stakeholders in producing reliable financial reports. It has brought significant attention and focus on internal controls at Senior Management levels for 'setting the tone at the top'. The internal control ownership has itself expanded from being primarily vested with the finance and accounting functions to the broader organisation – board of directors, senior management, business, audit, IT and operating management. Audit committees and Board of Directors are substantially more involved in overseeing the financial reporting processes and internal control environments while discharging their responsibilities. Audit firms have improved their relationships with audit committees, extensively trained their people on auditing internal controls, and enhanced their audit approach to focus on the evaluation of internal controls along with the financial statement audit. Auditing profession itself is being subjected to PCAOB oversight process and both SEC and PCAOB now have additional resources and authority to discharge their functions.
- PWC analysis of 225 organisations showed that they identified and remediated nearly 63,000 control deficiencies in total or approximately 275 control deficiencies per company. The Act has brought marked changes in behavior and attitude amongst key stakeholders - management teams, audit committees, boards of directors, investors, regulators and auditors. There is more focus and attention to maintaining effective systems of internal control and identifying and remediating internal control deficiencies before material misstatements occur.
- Section 404 highlighted significant weaknesses in IT security and also the issues associated with disparate IT systems. Another interesting observation was – many of the key controls were manual controls in spite of high technology investments. Going forward, there will be more focus on upgradation of existing transaction processing and accounting systems as well as financial reporting and analysis mechanisms. Significant investment (AMR research estimates the investments at USD 5.5 Billion) in upgradation of technology systems and tools and integration of diverse systems. Section 404 has provided the required impetus for upgradation of technology solutions.
- The remediation from Section 404 implementations have avoided possible material misstatements, improved the transparency and reliability of the financial information, reduced the likelihood of material frauds. 55 per cent of companies in FEI survey believe Section 404 gives investors more confidence in a company's financial reports, while the per cent is much higher at 83 per cent per cent of large companies (over $25 billion). Another interesting observation was – there was lack of standardisation of similar processes across locations, there were duplications and redundant controls. Such a critical analysis will help in simplification and standardisation of processes and ultimately, improvement in business processes.
- As regards cost-benefit analysis, it must be noted that the first year cost has been abnormally high – extra-ordinary time, effort, resource and investment was required for first time documentation (approx 25 per cent), testing and remediation (approx 15 per cent) as well as staff training. The benefits of Year 1 cost will accrue and realise in future years. Also, going forward, the investment may not be so high - 85 per cent of the organisations in FEI survey expect non-auditor expenditures to decrease (by an average of 39 percent) while 68 per cent believe that the primary auditor costs will also decrease (by an average of 25 percent). A more balanced cost-analysis can be done once the data for a longer period of time is available and that too taking into account 'normalised cost' and total benefits. Finally, there are intangible benefits—improved financial reporting process can assist investors in informed decision making and allocation of capital. Even, credit rating agencies are examining this aspect closely and have included it as a parameter in the rating process.

Comparison of SOX Provisions from an Indian Perspective

Corporate governance standards and the audit reports issued under the Companies Act in India require that organisations report on the Internal Controls Framework existing within the company.

As per Corporate Governance requirements, the management team is responsible for setting up and implementing an effective internal control system, commensurate with business requirements. Stock exchange listing requirements stipulate that the management include 'management discussion and analysis' (MD and A) reports on significant matters, including internal control systems and their adequacy. The Management has to report on the internal control and monitoring mechanisms put in place for financial statement assertions. Stock exchange listing requirements also require external auditors to certify on corporate governance compliance.

As regards the reporting under Companies Act, the external auditor is expected to plan and perform audits to obtain a reasonable assurance about whether the financial statements are free of material misstatements. The auditor will as a rule perform a sample testing of the evidence supporting amounts and disclosures, assess accounting principles and significant estimates made by the management and evaluate the overall financial statement preparation. The focus is not on internal controls but on a 'true and fair' view on financial statements.

Companies (Auditors' Report) 2003, requires the external auditor to report on various matters specified – fixed assets, inventories, transactions with related parties, public deposits, and so on. The report also requires the external auditor to specifically report on the adequacy of internal control procedures and the adequacy of the internal audit system and, whether, these controls are commensurate with the size of the company and the nature of its business.

As described above, while there is emphasis on internal controls, there is no strong thrust on internal controls as in the case of SOX. In India, the external auditor, as part of audit planning, does look into the significance of the amounts in financial statements and underlying risks of misstatement. But the Act does not require the organisations to record an elaborate internal controls document, test internal controls and keep the evidence thereof, nor is there a requirement for the auditor to specifically attest management assessment of internal controls. This difference in the Indian and American context can be partly due to the fact that India has not had any significant corporate debacles like in the US. India also does not have the history of legal suits against audit firms or management teams for corporate failures.

However, with the SEBI Committee recommendations on Corporate Governance in December 2003, the scenario is changing. The draft recommendations require CEOs/ CFOs to certify on the accuracy and completeness of financial statements and also on the existence and effectiveness of internal controls. This is similar to SOX Section 404; however, the major difference vis a vis Section 404 is that it is a mere certification from the management and not backed by external auditor attestation.

Conclusion

SOX has been criticised as a knee-jerk reaction to corporate scandals rather than a proper, well-thought out plan. Critics have also branded Section 404 as a 'bonanza' for accounting firms. However, the fact remains that it has brought significant changes in the attitude and behavior of all stakeholders which none of the past acts could accomplish. It has provided high visibility to internal controls which will ultimately result in the improvement in quality, reliability and transparency in financial reporting. This can only win back the investor trust and confidence, assist them in informed decision making and capital allocation and finally, strengthening the cornerstones of efficient capital markets.

Efforts are already underway in Europe and rest of the world to develop laws similar to SOX, 2002. ❐