



Challenges of Being Small in a Compliant World

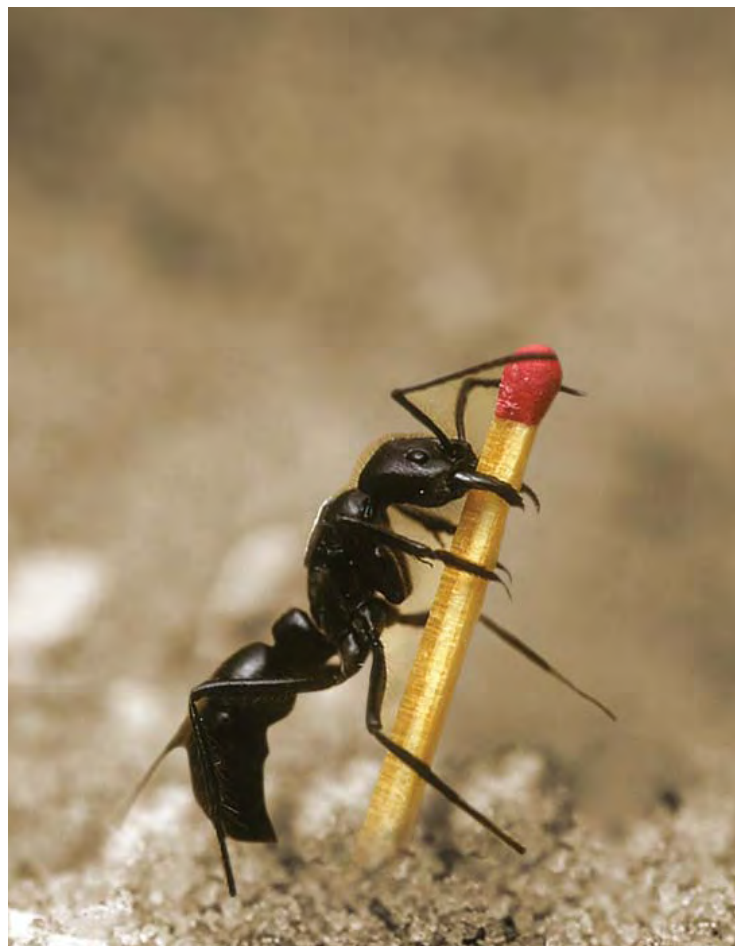
SOX Compliance for SMEs

An IT organisation, with well-defined internal controls, enables companies to identify and manage their IT related risks. The ability to manage and contain such risks is critical to ensuring compliance with regulations and mandates such as Sarbanes-Oxley Act (SOX). However, the understanding of SOX, and the implications of its Section 404, is still unclear, when it comes to Small and Medium Enterprises (SMEs). The article takes an in-depth look at how SMEs are affected by regulatory compliance, where they stand in achieving compliance targets, and why they should take SOX seriously.

■ BY SDA INDIA

US, early 2002. Public trust in the accounting practices of most publicly listed companies is at an all time low, thanks to a series of corporate and accounting scandals, such as those involving Enron and Tyco International. The government decides to step in, and in a desperate bid to reassure the people, passes the historic Sarbanes Oxley Act. That was five years ago. Today, Sarbanes Oxley—Sarb-Ox or SOX as it is popularly known—has become the sword that hangs over every CFO. Much has been spoken, written, and debated about how the Act is causing more economic loss than regaining trust, how the cost of compliance is affecting companies, and how companies can effectively catch up with the requirements. While large enterprises found solutions, hired experts and changed their way of functioning, Small and Medium Enterprises (SMEs) were largely left to fend for themselves, without much idea of how the Act really affects them.

This is now changing, as the need and advantages of compliance for smaller companies is gaining focus. “Smaller companies may find it difficult to address the IT control considerations that are expected under Sarbanes-Oxley. Therefore, it is important not a one-size-fits-all strategy, but instead risk-based approach and implement only those IT controls that are necessary and relevant in the circumstances,” says the report, IT Control Objectives for Sarbanes Oxley, Second Edition, a guide issued by the IT Governance Institute. In July 2006, the Committee of Sponsoring Organisations of the Treadway Commission



(COSO) also issued Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting, in a further effort to provide guidance for smaller companies looking at compliance. Let's take a quick look at why smaller companies should sit up and take notice of the Act.

Pulling Your SOX Up

Most smaller companies are exempt from the regulations because they are not public, or they do not deal with healthcare or financial issues. But that is hardly the complete picture. If you are an SME, that is listed, the implications of SOX are quite similar to those for large companies. Even if SMEs are not directly affected by the compliance rules, they may have to deal with it if they have clients facing the issue. For example, if a company is a supplier to a medical device manufacturer, the compliance requirements for the end product can be met only if the entire supply chain adheres to the regulatory requirements. In fact, the law mandates that regulated companies should ensure their suppliers meet compliance requirements by conducting supplier audits.

The Act is extensive, and going through the fine print can be quite a painful exercise. According to Frank Yam, Vice President of Information Systems and Audit Control Association (ISACA), the requirements of the much-discussed Section 404 can be simplified into five steps or components that the management needs to follow:

- Recognise the responsibility towards internal controls over financial reporting
- Choose an acceptable internal control framework, such as the Integrated Internal Control Framework, (also known as the COSO framework) or the COBIT framework
- Assess and evaluate the internal controls for efficiency
- Based on the evaluation, report on all the Material Weaknesses identified
- Hire external auditors to do the attestation report and the financial report

Makes compliance sound like cakewalk, doesn't it? The Act is lenient towards smaller companies when it comes to the deadline. Large enterprise were given time till November 2004, which means they have already been compliant for a little more than two years now. SMEs, on the other hand, have time till Dec 2007. The act has two parts—first being an internal assessment by the management of internal control, and then the certification by an external auditor. While the SMEs should have their internal controls in place by December 2007, the external audit can wait till December 2008.

Not Really a Cakewalk

While it has its own pluses, being small in an increasingly demanding, not to mention distrusting, world is not all that easy. When large enterprises themselves have found compliance to be a daunting task, the challenges for SMEs can be more. Ignorance has never been bliss, and the biggest crippling factor is that a lot of small companies do not have a good understanding of compliance. While the bigger companies can afford a legal and compliance department, smaller companies lack such sophistication. When there is a lack of understanding of what the requirements and expectations of SOX are, the chances of taking the wrong decisions increase.

To add to their woes, smaller companies usually would not have had focused internal controls in the past, which in turn converts to a weaker internal control environment. Audit departments are either non-existent, or involve a few individuals. So when they get to compliance, the management realises that those few individuals are not sufficient to finish all the assessment that SOX demands. Knowledge and skill levels are low at all levels in the organisation from a compliance perspective, and hiring external experts can dig a deep hole in a company's pocket.

Another challenge is that most SMEs follow procedures that are very informal, which do not hold well in a SOX-happy environment. The processes need to be formalised, which means implementing a change in the way control is practiced. These enterprises then need to make a lot of

Some companies, mostly smaller ones, that used to be publicly traded have de-listed and become privately held, because of the requirements of SOX compliance and the associated costs. Fewer than 20 per cent of the CFOs of companies large enough to go public, that have declined to do so, cite SOX as a reason that their companies remained private.



Frank Yam,
Vice President, Information Systems and Audit Control Association (ISACA)



“The mindset is to see compliance as a necessary evil and not to approach it as a positive value adding process. Companies look for quick fixes by ‘throwing people at problems’ and not for sustainable ways to build compliance in the DNA of the organisation”

Shankar Bhaskaran,
Director & Head of Marketing & Sales,
MetricStream India

changes, which means that the staff has to essentially change the way they practice controls. So the indirect implication is that the staff is going to feel the pain of having to go through a dramatic change in the way they practice their controls, and communication.

In the APAC region, the regulatory environment is still taking shape and companies are in the early stages

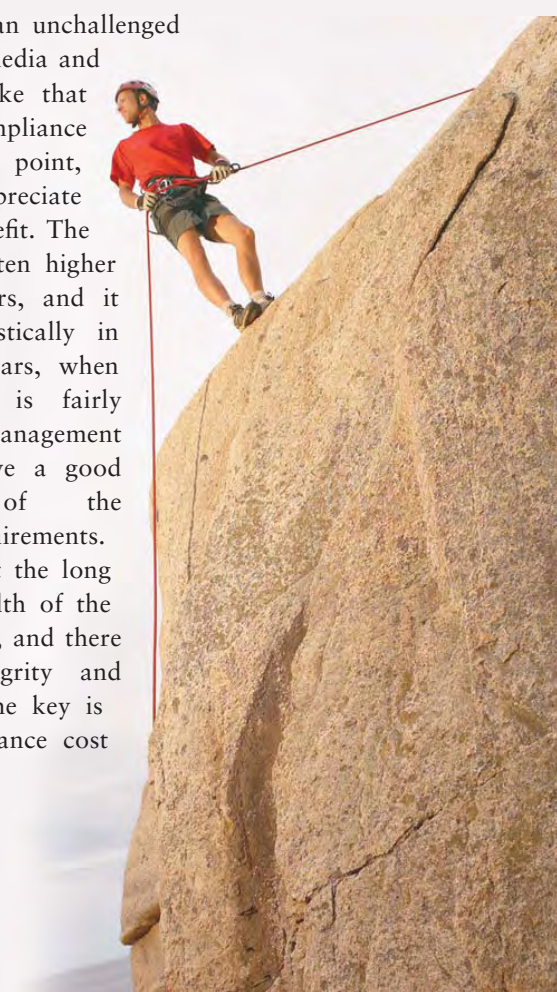
of deciding their compliance strategies and approach. Although there are regulations like J-SOX (in Japan) or A-SOX in (Australia), the regulatory frameworks and enforcement programs are not well defined by governments and not in sync with the times, says Shankar Bhaskaran, the Director & Head of Marketing & Sales, MetricStream India. “The mindset is still to see

Meeting the Challenges

Compliance is like a large chandelier in the middle of a ballroom. Everyone in the room sees it, but each from a different angle. So while the law may be the same, the way smaller companies react to and achieve compliance can be quite different. Management of smaller companies tends to have a hands-on approach, wider spans of control, and the ability to provide ongoing monitoring through direct relationships with key personnel, vendors, customers, and capital providers. This can create opportunities whereby controls may be less formal without decreasing their quality. It is important not to take the one size fits all strategy.

The first requirement is to understand the exact requirement and implications of SOX. The management will then have to find resources within the organisations to start the assessment. The important factor here is that these resources need to understand how to implement the required internal control and framework, and further, to perform the assessment and testing of the controls that are in place. This is where most small enterprises falter—if they do not have adequate resources within the organisation, then the need to hire external consultants arise, which in turn leads to increased cost. The additional cost also comes in the form of fees to be paid to the external auditors to do the attestation report.

While there is an unchallenged consensus in the media and the companies alike that the cost of compliance is its biggest pain point, they often fail to appreciate the associated benefit. The extra costs are often higher in the initial years, and it comes down drastically in the subsequent years, when the environment is fairly stable, and the management and the staff have a good understanding of the compliance requirements. The benefit is that the long term financial health of the company increases, and there is increased integrity and customer trust. The key is to achieve compliance cost effectively.





Management of smaller companies tends to have a hands-on approach, wider spans of control, and the ability to provide ongoing monitoring through direct relationships with key personnel, vendors, customers, and capital providers.

compliance as a necessary evil and not to approach it as a positive value adding process. Companies look for quick fixes by ‘throwing people at problems’ and not for sustainable ways to build compliance in the DNA of the organisation.”

But the biggest challenge by far is the cost, and this is where large and small companies are taxed alike. A March 2005 survey by Financial Executives International found that in the first year, SOX compliance costs averaged USD 4.36 million per company, and large companies with more than USD 5 billion in revenue spent more than USD 10 million per company. For small enterprises, with their limited funding options, it can be quite a challenge to address the cost of compliance. But according to Antony Ung, Business Development Manager at CA, the cost factor can be slightly less taxing in the APAC region, as compared to Europe or North America.

COSO to the Rescue

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) has released the Second Edition of the IT Control Objectives for Sarbanes Oxley, which details the new COSO Framework, which is called the Risk Management Framework. The original COSO Framework, popularly known as the Integrated Internal Control Framework, had five components—Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring.

The second framework issued by COSO is the

Enterprise Risk Management Framework, which has eight different sections. Most of these sections are similar to the ones before, except for two parts, which are the Control Environment, now called the Internal Environment, and the Risk Assessment, which is now broken down into four components.

- Objective setting
- Event Identification
- Risk Assessment
- Risk Response

While the Integrated Internal Control Framework has become a de facto framework used by companies for internal control to comply with SOX, the Enterprise Risk Management Framework has not been that widely adopted. In fact, a study released by Institute of Management Accountants (IMA), says that two of the key cost drivers for public companies complying with Sarbanes Oxley Section 404 (SOX) requirements are lack of practical management implementation guidance and incomplete nature of the COSO 1992 framework in assessing effectiveness of internal controls over financial reporting. But Yam says that new guidance issued by COSO, which is the Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting, is the answer to this issue. This document does not aim to replace the original framework, but rather a spin off. It provides guidance in using the framework in designing and implementing cost-effective internal controls over financial reporting.

Meeting Tomorrow’s Needs Today

According to Ung, since it is not mandatory for SMEs to comply, it becomes more of a business policy decision. “SOX compliance is a necessity to gain that competitive edge, while competing with larger enterprises globally.”



KEY AREAS OF COMPLIANCE SPENDING

- Documentation of key processes (finance, operations and IT) and change management, (DMS)
- Documentation of internal controls and change management
- Document Management Software (DMS) and SOX software
- Design and testing of controls
- Consultants, internal audit, Audit software, Controls automation software, Security software and ERP/analytics software
- Remediation
- Attestation



INTEGRATED INTERNAL CONTROL FRAMEWORK



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 control environment primarily addresses the entity level. However, additional emphasis on business alignment, roles and responsibilities, policies and procedures, and technical competence.

Risk Assessment

Risk assessment involves management's identification and analysis of relevant risks to achieving predetermined objectives, which form the basis for determining control activities. Risk assessment may occur at the entity level (for the overall organisation) or at the activity level (for a specific process or business unit).



Control Activities

Control activities are the policies, procedures and practices that are put into place so that business objectives are achieved and risk mitigation strategies are carried out. Without reliable information systems and effective IT control activities, public companies would not be able to generate accurate financial reports. COSO identifies two broad groupings of information system control activities:

Application controls—embedded within software programs to prevent or detect unauthorised transaction
General controls—needed to support the functioning of application controls. Both are needed to support accurate information processing and the integrity of the resulting information used to manage, govern and report on the organisation.



Information and Communication

Information is needed at all levels of an organisation to run the business and achieve the entity's control objectives. However, the identification, management and communication of relevant information is a challenge. The determination of which information is required to achieve control objectives, and the communication of this information in a form and time frame that allow people to carry out their duties, support the other four components of the COSO framework.



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. Increasingly, IT performance and effectiveness are being continuously monitored using performance measures that indicate if an underlying control is operating effectively.

Source: IT Control Objectives For Sarbanes Oxley, 2nd Edition



“It is not mandatory for smaller companies to comply. It is a more of a business policy decision. SOX compliance is a necessity to gain that competitive edge, while competing with larger enterprises globally.”

Antony Ung,
Business Development Manager, CA

Moreover, if the company is looking to be acquired by a larger enterprise, then compliance is definitely an advantage. Today, stock markets are highly sensitive to the compliance issues of a company. Hence the value of a company from an acquisition perspective is directly tied to how well it manages its risk and regulatory compliance issues. If the acquiring company needs to be compliant, they would definitely be looking into the internal control and compliance status of the acquisition target. In fact, Yam claims he has been quizzed about a smaller company’s compliance status by the financial advisors (read investment banks) of the acquiring company. Compliance may not be such a bad idea, even if the company is not publicly listed.

But if, as a company, you have not made up your mind to plunge head on into the compliance race, there still are a few steps that can be taken to prepare the company, in the wake of mandatory compliance. SMEs in particular, need to take action to reduce the cost involved, and they need effective planning to make their enterprises ‘compliant’. By ensuring that their enterprises are ready

for SOX, companies can be prepared in case of mandatory compliance. Bhaskaran enumerates five steps that SMEs can take to get themselves SOX-ready, while keeping the costs low:

- Decentralise SOX compliance responsibility by shifting compliance tasks and activities downstream to process owners and line managers
- Rationalise controls to avoid excessive and redundant documentation and testing
- Automate documentation, change controls, testing and evaluations to reduce the manual effort and consulting fees
- Train employees to ensure required level of compliance knowledge and skill in the organisation
- Ensure clear visibility into the compliance process and into the changing regulatory environment

Conclusion

US President, George W. Bush, signed the Sarbanes Oxely Act stating it included “the most far-reaching reforms of American business practices since the time of Franklin D. Roosevelt.” And to be sure, post Sarbanes Oxley, the markets around the world are expecting more from the management teams of all companies, large or small, in their corporate governance and their role in setting up a good and effective system of internal control. This expectation is not going to be reversed in the future, regardless of what the laws and regulations demand.

The Act may still change to be more considerate towards smaller companies, but the intent behind it—to improve overall corporate governance—is unlikely to change.

The core idea of SOX is that investors and management should be fully aware of the risks that a company faces and should put controls in place to mitigate those risks. Though SOX may not directly apply to private companies, the concepts of risk management and mitigation are relevant to SMEs as well and affect the confidence of stakeholders such as customers, partners, debtors, and institutional investors.

SMEs need to realise that SOX is not a necessary evil. It is a necessary good. With good corporate governance, a company can assure its customers, partners, and investors that their money is in good hands, and that the future is secure, and stable. Bhaskaran has the final word, “Regulatory compliance, either as SOX or as any other regional law, is here to stay. It is the right time to start understanding the laws and to build a long-term, sustainable compliance strategy.” ■