Deloitte.

Internal Financial Controls
Board of Directors - Get comfortable in the cockpit

August 2015

For private circulation

Choosing the right framework for Internal Financial Controls

The Companies Act 2013 infused significant rigor by introducing many new provisions for Indian companies in its pursuit to harmonize our governance led regulations with global standards. One of the more widely discussed requirements of the Act has been around Internal Financial Controls (IFC), with newer roles and accountabilities defined for the board, audit committee, statutory auditors, and the management.

Indian companies are expected to provide assurance about the soundness of IFC, elaborated as follows:

- For listed companies, the Companies Act 2013 defines the term IFC very widely as the policies and procedures adopted by the company to ensure orderly and efficient conduct of its business, including adherence to company's policies, safeguarding of its assets, prevention and detection of frauds and errors, accuracy and completeness of accounting records, and the timely preparation of reliable financial information. The management would therefore need to identify and document financial and non-financial controls, assure the boards of the adequacy of such controls and also demonstrate results of testing operating effectiveness of such controls.
- For unlisted companies, the Directors' Report for FY 2014-15 would have to disclose adequacy of controls related to financial statements.
- From FY 2015-16, for both listed and unlisted companies, it is mandatory for statutory auditors to make their observations on operating effectiveness of internal financial controls.

This in other words means that the boards of directors, who so far were looking at the CEO and CFO of the organization as a pilot of the plane for a safe flight, are now required to enter the cockpit, familiarize themselves with various levers, dials, instruments, and dashboards that exist and ensure they are operating effectively by asking the right questions. For directors who are on multiple boards the problem is more complex. They need to adjust themselves to different size and makes of planes i.e., the companies whose boards they serve on. To simplify the journey and to make it safer, the boards and management need to identify and agree on a standard global navigation system i.e., a widely adopted Internal Controls framework and then design internal mechanism to align with it, i.e. customize and adopt the framework.

The Companies Act 2013 requires the board of directors to be familiar with the Internal Financial Controls and ask the right questions

There are well-known standards set by bodies such as ISO for various business processes, Basel committee standards for banks and COBIT for Information Technology. The Companies Act has not prescribed any standard to be followed by Indian companies for IFC. While this gives companies the freedom to choose their approach, they also find the task that much more difficult as choice of framework/standard has to meet the unique company requirements and at the same time the board must be convinced of its robustness and the auditors should be able to rely and find tangible evidence of its working. One such widely used Internal Controls frameworks globally is the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Today, COSO 2013 is the flagship and overarching framework, recognized by regulatory standard setters and trusted by several US-listed companies as their reference framework of choice. The framework has superseded COSO's 1992 framework as of Dec. 15, 2014. It is wide and comprehensive in its coverage,

As there are no specifications prescribed by the Act with respect to adopting a standard, it becomes incumbent on companies to choose a standard

- which meets the unique requirement of the companies
- whereby the boards are convinced of the robustness of the standard and
- whereby the auditors are able to rely on the standard and find evidence of its effective working.

encompassing the overall internal controls of an enterprise as well as its financial controls and also controls for financial reporting. The framework states 17 principles across five components- (1) Control environment (2) Risk assessment (3) Control activity (4) Information and communication and (5) Monitoring and various Points of Focus (PoF) within each of the principles.

Many Indian companies are looking at COSO as the framework of choice for implementation of internal controls and a few are already transitioning to it. When evaluating internal controls using the COSO framework, it is recommended that organizations need to look at the framework in an integrated manner and ensure that all 17 principles are conformed to.

COSO 2013 framework- To adopt or not to adopt

India has a large population of promoter-driven companies which are often guided by the 'tone at the top'and may have their own stipulated and tested measure of internal controls. In many cases, the involvement of the management through what may be touted as a relatively 'less formal' set of controls may actually prove sufficiently effective. The reality is however that although effective in the context of such a company, the effectiveness now needs to be demonstrated to the directors who are not involved in day-to-day operations and auditors who would evaluate it based on tangible evidences. This makes a stronger case for adoption of a framework that can bring the directors, the management, and the auditors on the same page.

When evaluating internal controls using the COSO framework, organizations need to look at the framework in an integrated manner and ensure that all 17 principles are conformed to

While referring to the COSO 2013 framework, Indian companies would typically reflect on the following points:

Applicability – Can our company also adopt it?

Private companies – We are a private company; can we use it too?

Approach - How should we approach COSO 2013? Does the COSO framework provide guidance?

Implementation – Does the adoption of COSO require elaborate systems and structures at the organization and board level for the effective working of the controls?

Economics –Do the benefits justify the costs?

Conflicts – Will Segregation of Duties (SOD) give rise to conflict especially if we are have a small or medium organization?

One size doesn't fit all- COSO framework is no different

COSO recognizes that applying the framework can and should differ across different companies in accordance with their unique operating environments.

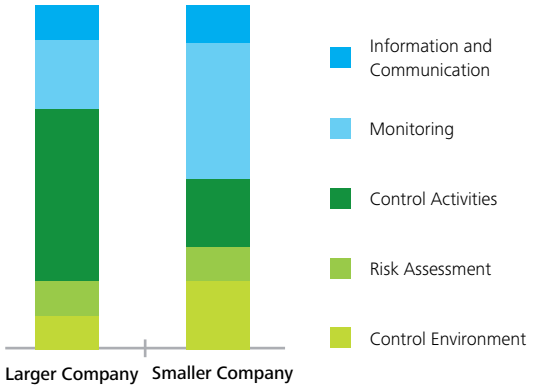
Smaller companies are defined based on company characteristics rather than revenue terms which include the following:

- Simple product line and processing
- Founders or a small group of owners who dominate management of the business
- Wider management spans of control
- Economic strategies that often encompass acquiring services on a variable-cost basis as
- Defined geographic concentration in either production or sales

How Indian companies can use this framework components to achieve effective internal control

There are five components which a company need to focus on while implementing the COSO 2013 and can assign weightage to each of the areas depending on the unique requirement of the organization. The chart indicates possible weightages usually assigned to the five components in the framework which may change depending upon the size of the company. At a foundational level, all the components will need to be functioning as part of the company's IFC strategic framework, but companies must use discretion to assign the mix rather than a straightjacket approach to adopting the COSO 2013 framework.

The smaller companies may need to have greater emphasis on control environment and monitoring as opposed to control activities. However, activities under these components need to be structured, well laid out, and demonstrable to compensate less formal control activities.



COSO recognizes that applying the framework can and should differ across different companies in accordance with their unique operating environments

Your COSO implementation strategy requires a judgement call, not a straightjacket approach

The COSO framework is principles-based. It is not a checklist implying that the same set of controls must be implemented uniformly in every company. Companies that focus on complying only with the idiomatic 'letter of the law' and not necessarily its spirit will fail to derive the desired value. COSO acknowledges the philosophy of having a controls framework commensurate with the nature and size of the company. The inability to customize your COSO implementation strategy to the needs of your organization can result in a quagmire of epic proportions in the form of bloated controls, heightened expenses and unnecessary complexity. Exercising awareness and judgement is of paramount importance to decide on how to adopt COSO 2013 framework considering organizational characteristics.

Five key components of COSO

1. Control environment
2. Risk assessment
3. Control activity
4. Information and communication
5. Monitoring

Let us look at each of the five components of the framework and understand illustrative approaches that smaller vs. large organizations can adopt:

1. Control environment

This component is the foundation on which all other components of internal controls rest. Needless to say, there is a clear correlation between senior management demonstrating commitment to ethical business practices and the effectiveness of internal controls. In companies where a clear 'tone at the top' is established, the success rate of implementing, and the monitoring effectiveness of internal controls also increases.

For instance, one requirement of COSO is that organizations are required to maintain an Integrity and Ethics policy, which will need to be demonstrated irrespective of the size of the organization. However there could be some differences as illustrated below:

Illustrative controls for large organization	Illustrative controls for smaller organization
• Publishing their Integrity and Ethics policy on the company website • Sharing with employees and taking confirmation on adherence • Include in contracts with service providers, and take their concurrence, etc.	• Display in the premises • Include reference in appointment letter • Share with service providers and take their concurrence

For the success of implementation and the effectiveness of internal controls, the tone at the top matters

2. Risk assessment

Risk assessment is an essential step in building effective control environment. Organizations need to identify what are the inherent risks in its business and financial reporting processes and then design controls with right mix of people, activities and technology to mitigate those risks. Organizations should build a fortress of strong controls around areas with high inherent risk, as the risk goes down to medium to low, it should get reflected in the nature of controls implemented. The objective of control is to mitigate risk and hence, as a rule, the cost of control should never be more than the risk itself. Also, risks are dynamic and hence the risk assessment exercise should be carried periodically. COSO framework suggests that the organization should concentrate its risk assessment on 1) financial reporting, 2) fraud risk, and 3) internal and external factors.

As an illustration, let's look at fraud risk and how it can be implemented in small versus large organizations. The Fraud Risk assessment evaluates components of incentives, pressures, opportunities, attitudes, and rationalizations. The extent of these varies significantly with scale and size of the organization, its employee base, its vendor and customer base, etc.

Illustrative controls for large organization	Illustrative controls for smaller organization
• Mandatory leave, periodic job rotation • Vendor assessments, audit of vendors, pricing/discount controls • Related party transactions, etc.	• Periodic physical verification to address theft of material • Signed contracts to formalize oral arrangements, etc. • Control over banking transactions

3. Control activities

The control activities are derived from the risk assessment process. Organizations should identify key controls that will help in mitigation of identified risks. Whether the organization is large or small, the main essence of control is around authorizations and approvals, verification, reconciliation, business reviews, and segregation of duties. The key differentiator for large organizations is the use of technology to manage the scale and have more automated controls as opposed to manual. Let us see some choices of control activities for large versus small organizations.

Illustrative controls for large organization	Illustrative controls for smaller organization
• Stronger segregation of duties • Formal SOPs • ERP including GRC solutions, etc.	• Management reviews • Manual controls • Higher senior management direct supervision

4. Information and communication

In today's context, information plays a very vital role. The key is quality of information generated and the quality is assessed through its accessibility, correctness, sufficiency, currency, validity, timeliness, etc. while these characteristics remain unchanged for large and small organizations, the larger organization generates huge amount of information and hence needs sophisticated systems to manage it whereas smaller organization can control this easily without such high-end systems. Similarly, while essence of communication would be similar, larger organization needs to develop different lines of communication considering higher number of recipient of such information. Some examples for large versus small organization under this component are as follows:

Illustrative controls for large organization	Illustrative controls for smaller organization
• Internal communication through various channels i.e., mails, webcasts, townhalls, etc. and across various departments • Specific cell to take charge of external communication including to regulators, media, stock exchanges, etc. • Reliable systems, information security controls using standards such as ISO 27001, etc.	• Weekly management meetings, physical visits by MD/CEO to plants/ operations and meeting employees • Physical controls over data i.e., minutes of meeting, etc.

Whether the organization is large or small, the main essence of control is around authorizations and approvals, verification, reconciliation, business reviews, and segregation of duties

5. Monitoring

In a smaller organization, monitoring plays a vital role in ensuring internal controls are implemented and operating effectively. The organizations needs to give careful consideration to ongoing and separate evaluations.

Illustrative controls for large organization	Illustrative controls for smaller organization
• Ongoing evaluations are automated and exceptions are reported and evaluated for appropriate approvals • Separate evaluations are conducted by experts either internal or external • Monitoring of operations at third-party processing centers	• Higher emphasis on ongoing evaluation • Separate evaluations are carried out by independent personnel or internal audit itself • Higher senior management direct supervision

Summary

The COSO 2013 framework requires organizations to adhere to all 17 principles. However the framework provides flexibility in terms of the controls that are required to address the principles. Organizations, based on the size and nature of the operations, need to implement controls that will meet their requirement.

Like every commercial aircraft will have engine, fuel, hydraulic and electrical systems, navigation and radio but they will significantly differ from one make and model to another, every company's internal control environment can be structured on the five components of COSO framework but companies can design their own controls within the specified guidance. While still relying on the CEO and the executive management for a successful flight, directors should familiarize themselves with the basic construct of the organization on whose board they serve and develop an instinct to spot a malfunctioning system and direct the management to correct it.

Five key questions which directors may ask

1. How would management demonstrate to the board the existence, adequacy, and effectiveness of controls?
2. Is the management intending to implement a recognized internal control framework under which the program for compliance will work?
3. Is the board comfortable with the proposed framework? Can it be customized considering organizations size, complexity, nature of business, etc.?
4. What skills are required to implement and sustain such a program? Does the organization have the skills?
5. What is the dashboard that will provide the directors with information and enable them to direct the management?

Contacts

Abhay Gupte
Senior Director
Deloitte Touche Tohmatsu India Pvt Ltd
agupte@deloitte.com
Phone: +91 22 6185 4360

Sachin Paranjape
Senior Director
Deloitte Touche Tohmatsu India Pvt Ltd
saparanjape@deloitte.com
Phone: +91 22 6185 4903