

Reporting on Internal Controls

Developing a top-down, risk-based approach to internal controls

A top-down, risk-based approach is based on the premise that not all accounts, transactions, and risks are equally important. This approach focuses control resources on the areas identified as being of greater risk because of their relative quantitative significance and other related concerns, including the nature of the business; the inherent riskiness of transactions, processes, controls, and technologies; and the effectiveness of the organization's human resources.

Companies should also apply a balanced holistic view in their design of controls. If, for example, compliance efforts are initiated through a bottom-up approach that treats all controls equally regardless of the underlying risk profile, the company will end up testing of a large number of controls at the routine level (which usually address relatively lower risks), which will require a bloated and disproportionate control structure that devotes the majority of time, effort and resources to controls over routine transactions, and allocates relatively little time, effort and resources to the high risk controls and entity level controls.

A "top-down" approach begins with a risk assessment that includes:

- Developing a thorough understanding of a company's financial reporting risks
- Identifying and considering the design of controls, starting with company-level controls and proceeding down to the identification of significant accounts, key groups of transactions and related processes; and
- Evaluating individual controls
- When control rationalization is approached from this vantage point, it better enables the compliance program to focus on the most appropriate areas and promotes a process through which "in scope" areas receive a level of attention commensurate with their relative level of risk.

Reporting on audits of internal control

In the United States of America, the SEC and the PCAOB have worked together to make the internal control provisions related to SOX section 404 more effective and more cost efficient. The Institute of Chartered Accountants of India has issued Standard on Auditing (SA 315), Identifying and Assessing the Risk of Material Misstatement through understanding the Entity and its Environment which provides guidance on auditor's responsibility to identify and assess the risk of material misstatement in the financial statement, through understanding the entity & its environment, including the entity's internal controls.

When performing an engagement in accordance with this auditing standard, the auditor shall perform risk assessment procedures to provide a basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels. The auditor is expected to obtain an understanding of internal controls relevant to auditing which in most of the cases are likely to relate to the financial reporting. The auditor is also supposed to obtain an understanding on whether the entity has a process for identifying business risks relevant to financial reporting objectives. Further in understanding the entity's control activities, the auditor shall obtain an understanding of how the entity has responded to risks arising from its information technology framework and applications.

The auditor shall evaluate the design of financial reporting controls and determine whether they have been implemented, by performing procedures in addition to inquiry of the entity's personnel. The auditor shall communicate material weaknesses in internal control identified during the audit on a timely basis to management at an appropriate level of responsibility, and, as required by SA 260 (Revised), "Communication with Those Charged with Governance", with those charged with governance (unless all of those charged with governance are involved in managing the entity).

Action plan for Indian reporting issuers

Deloitte has developed a five-step action plan to help public companies in India to certify the effectiveness of their internal control systems in line with the Clause 49 requirements.

- **Control framework and entity level controls.** Decide on and implement a suitable control regime. Companies should take a "top down" approach that starts with the identifying business, disclosure and financial reporting risks.
- **Identify principal business risks.** Principal business risks should include disclosure and financial reporting risks so these risks and the systems put in place to manage and control them can be properly aligned. CEOs and CFOs need a reliable risk identification process in order to make them reasonably assess whether the design of ICFR adequately addresses all principal disclosure and financial reporting risks. Such a risk identification process also provides a basis for ensuring that the various risk disclosures provided in the financial statements, Management Discussion & Analysis (MD&A) and the disclosure of corporate governance practices are complete, fair and informative to the investors.
- **Effectiveness of the CEO/CFO certification process.** Companies should examine their process for evaluating the design and effectiveness of ICFR. This examination should include "sub certifications" and any other processes that the CEO and CFO may have put in place to provide them with the information and assurances they need to certify the content of the issuer's filings. Any weaknesses in the company's certification process should be identified and corrected as this process will serve as the foundation for certifying the design and evaluation of ICFR.
- **Preliminary identification of potential weaknesses in control.** CEOs and CFOs should consult with other members of management including internal audit, legal counsel and external auditors to identify all potential control weaknesses that could indicate possible design weaknesses in ICFR. Any material design weaknesses that are not remediated will likely have to be publicly disclosed in the MD&A. The early identification of potential weaknesses in ICFR provides companies with the opportunity to decide on the best corrective action, not only to avoid disclosing a material weakness in ICFR and describing the company's disclosure controls as "ineffective" in the MD&A, but also to better manage the business.
- **Board and audit committee responsibilities.** Audit committees should review their risk and control related responsibilities, and the information and assurance they require in discharging those responsibilities. The charters of the board of directors and the audit committee must clearly articulate the division of responsibilities between the board and the audit committee.

To explore these ideas further, contact your

Lead Client Service Partner

or

Abhay Gupte

Director, Deloitte Center for Corporate Governance, India

Tel.: + 91 (22) 6681 0600

E-mail: agupte@deloitte.com

In this material Deloitte refers to Deloitte Touche Tohmatsu India Private Limited (DTTIPL), a Company established under the Indian Companies Act, 1956, as amended.

DTTIPL is a member firm of Deloitte Touche Tohmatsu, a Swiss Verein, whose member firms are legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

This material prepared by DTTIPL is intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s). Further, the views and opinions expressed herein are the subjective views and opinions of DTTIPL based on such parameters and analyses which in its opinion are relevant to the subject.

Accordingly, the information in this material is not intended to constitute accounting, tax, legal, investment, consulting, or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser. None of Deloitte Touche Tohmatsu, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this material