The newsletter for Audit Committee members in Thailand

# On Board*

Issue 2: March 2006

## In this issue



PRICEWATERHOUSECOOPERS

*connectedthinking

# Editors comments

Welcome to the second edition of the PricewaterhouseCoopers Audit Committee newsletter.

Our first article focuses on monitoring the integrity of financial reporting - with the reporting season upon us, the article provides practical tips on what to look for when reviewing the integrity of corporate reporting.

Our next two articles cover fraud and business continuity planning and aim to stimulate thought on what exactly is the role of the audit committee in these two areas, and how can the committee position itself to discharge its responsibilities effectively.

Our final article features the results from PwC's 9th Annual Global CEO survey on "globalisation and complexity". The article highlights the key challenges facing CEOs in these areas and in doing so, provides audit committees with valuable insights in areas that will undoubtedly impact their organisation's responses to risk management and internal control.

We hope you will find this edition helpful and interesting. We would also welcome any feedback from you on ways in which the newsletter might be improved for future editions.

Varunee Pridanonda
Partner

# The contributors from our Corporate Governance, Risk Management, Internal Control and Internal Audit team


**Varunee Pridanonda, partner,**
*varunee.pridanonda@th.pwc.com*
Tel: 66 (0) 2344 1282

**Marius Kunneke, director,**
*marius.kunneke@th.pwc.com*
Tel: 66 (0) 2344 1025

**Svasvadi Anumanrajdhon, partner,**
*svasvadi.anumanrajdhon@th.pwc.com*
Tel: 66 (0) 2344 1111

**Suntaree Leepakorn, director,**
*suntaree.leepakorn@th.pwc.com*
Tel: 66 (0) 2344 1061

**Richard Wilkins, director,**
*richard.wilkins@th.pwc.com*
Tel: 66 (0) 2344 1190

**Michael Haddon, director,**
*michael.haddon@th.pwc.com*
Tel: 66 (0) 2344 1031

# Monitoring the integrity of financial statements

At this time of year, Audit Committee agendas in organisations with December financial year ends are typically focused on financial reporting and disclosure matters. In this article, we provide Audit Committees with guidance on the type of questions they need to ask when reviewing the integrity of the company's financial statements and other formal announcements relating to financial performance.

By undertaking a rigorous review of the financials (and exercising a degree of scepticism with respect to matters of financial reporting), the Audit Committee will be better placed to manage expectations. Increasing stakeholder activism is leading to more difficult and probing questions to Boards, particularly at shareholders, annual meetings.

Furthermore, the credibility of financial statements has been seriously damaged in recent years with numerous financial reporting scandals hitting the headlines across the world. All this adds up to more a more challenging time for Audit Committees.

**Mis-statement of Financial Information - What are the indicators?**
There are a number of indicators that can warn Audit Committees that the risk of mis-statement may be high:

- A significant portion of management's compensation is in the form of bonuses, contingent upon achieving certain financial results or share prices.
- Financial performance significantly outperforms the economy and industry sector.
- Domination of management by a single person or small group, without compensating controls by the Board of Directors.
- Frequent disputes between the current or prior auditor with management on accounting, auditing, or reporting matters.
- Restrictions on the auditor that inappropriately limits access to key people or information.
- Inability to settle current liabilities while reporting net positive earnings.
- Significant related party transactions beyond the ordinary scope of business.
- Adverse consequences on significant pending transactions if poor financial results are reported.
- Increasingly aggressive accounting policy changes, e.g. revenue recognition, asset depreciation, and intangible asset capitalisation.
- Inadequate time allowed for the Board of Directors and the Audit Committee to evaluate the financial reports and disclosures.

The opportunity for mis-statement also increases significantly in the absence of adequate and effective corporate governance processes, enterprise risk management framework and processes, systems of internal control, internal audit and adequate segregation of duties and supervision.

**What to look for - areas that need special attention**
In addition to the above mis-statement indicators, audit committees should also raise questions with the internal & external auditors and management in areas such as:

- Off-balance sheet transactions, including assets and liabilities.
- Infrequent, complex, abnormal and one-off transactions.
- Derivative transaction recording and valuations.
- Transaction recording and disclosure that requires judgement, for example provisions, intangible asset valuations, etc.
- High number of year-end adjustments.
- Significant increases from prior years in different types of revenues and working capital assets, or significant decreases in expense items and working capital liabilities.
- Cash and revenue growth not following the same trend.
- Industry specific accounting issues.

**How to minimise the risk of mis-statement?**
Audit Committees must use their combined experience and skill to identify and interpret all of the indicators noted above. In addition, further assurance can be obtained by:

- Understanding how management and the external auditors assess the risk that the **financial statements** may be materially misstated.
- Reviewing with management and the external auditors those "grey areas" requiring **significant judgement**.
- Ensuring that the company has an adequate **internal control framework** by obtaining management's and the Board's view on whether they believe the internal controls are effective.
- Ensuring the independence of the **external auditors.**
- Reviewing and approving the scope of **internal audit** activities.
- Overseeing management processes for identifying and managing enterprise risks, financial reporting risks, legal and regulatory compliance risks, and operational risks.

Increasing obligations require substantial time and commitment from directors and Audit Committee members to comply with financial reporting standards, legal and regulatory compliance and sign-offs for just about every facet of the business. The Audit Committee can fulfill its role and protect stakeholders by ensuring that all the right questions are asked of those people responsible for the preparation and sign-off of financial information.

# Reducing the risk of fraud - how robust is your organisation's fraud prevention and detection framework?

**Fraud risk is very real** - PwC's recently issued Global Economic Crime survey for 2005 revealed some interesting results. Overall, it is clear that fraud risk, and the incidence of fraud, are very real issues facing most businesses.

In terms of fraud incidence, 45% of companies worldwide have fallen victim to economic crime in the last two years, and no particular industry appears to be safer than any other. If we look to the results from the Thai section of the survey, the highest numbers of frauds were in the categories of asset misappropriation (46%), corruption and bribery (44%), and false pretences (35%).

**What do we mean by fraud?**

Fraud is a broad concept that refers generally to any intentional act committed to secure an unfair or unlawful gain. Financial fraud typically falls into the following four broad categories:

1. Fraudulent financial reporting - most schemes involve earnings management, arising from improper revenue recognition, and the overstatement of assets or understatement of liabilities;

2. Misappropriation of assets - external and internal schemes, such as embezzlement, payroll fraud, and theft;

3. Expenditure and liabilities for improper purposes - commercial and public bribery, as well as other improper payment schemes; and

4. Fraudulently obtained revenue and assets, and costs and expenses avoided - schemes where an entity commits a fraud against its employees or third parties, or where an entity improperly avoids an expense, such as tax fraud.

**A proactive approach to risk and controls?** - When looking to fraud controls, despite the growing confidence that the companies surveyed have in their risk management systems, a significant level of fraud (34%) is still detected by chance, for example through tip-offs.

This probably reflects the fact that to date, many companies have taken a more reactive approach to dealing with fraud - relying more on basic trust for prevention and, if a fraud incident arose, dealing with it as best they can. Such an approach is no longer adequate in today's more demanding business and regulatory environment.

**What should the next steps be?** - Whether driven by new laws and regulations or market based expectations, Boards and Audit Committees must ensure that there are effective risk management and internal controls in place to prevent fraudulent financial reporting - and to detect it on a timely basis when it does occur. Companies are recognising that there is need to strengthen their anti-fraud programs.

Compared to the results from PwC's 2003 Economic Crime survey, many respondents appear to have significantly increased their efforts to mitigate the risk of economic crime. The more control measures a company puts in place, the more incidents of fraud it will uncover, and the less likely it is that the company will suffer significant ongoing "collateral" damage to its brand and reputation.

For Thailand, many companies pointed to internal audit, internal controls, and ethics programs as areas where they will pay more attention in the next two years in order to prevent economic crime.

**What does a good anti-fraud program look like?**

A company with a good anti-fraud program will have as a minimum, the following five characteristics:

1. A code of conduct designed to deter wrongdoing and promote honest and fair conduct;

2. An ethics/whistleblower hotline designed to encourage employees to communicate concerns without fear of retribution;

3. A hiring and promotions policy which looks to ensure only suitably qualified individuals with the right background, experience, and integrity are working at all levels in the organisation;

4. Effective investigation and remediation processes that promote timely and objective responses to control deficiency or incidents of suspected, alleged, or actual fraud; and

5. Strong oversight of fraud controls by the audit committee (and board).

**The Audit Committee's role** - By adopting a structured approach to the oversight of the fraud prevention and detection program, the audit committee will better appreciate the company's risk profile and management's approach to managing the risks and in doing so, support the main board to discharge its fiduciary responsibilities.

**What is the specific role of the audit committee in an anti-fraud program?**

The audit committee's key role is one of oversight and to fulfil this role, it must systematically and periodically review the following:

1. Management's anti-fraud program and controls, including its identification of fraud risks and implementation of anti-fraud measures;

2. The potential for management override of controls or other inappropriate influence over the financial reporting process;

3. Mechanisms for employees to report concerns;

4. Receipt and review of reports describing the nature, status, and eventual disposition of alleged or suspected fraud and misconduct;

5. An internal audit plan that addresses fraud risk and a mechanism to ensure that the internal audit can express any concerns about management's commitment to appropriate controls or report suspicious or allegations of fraud; and

6. Involvement of other experts - legal, accounting, and other professional advisors - as needed to investigate any alleged or suspect wrongdoing brought to the committee's attention.

**In summary** - A robust, integrated anti-fraud program focussed on prevention and detection can create large cost savings that go directly to the bottom line and can significantly improve the company's financial performance and its reputation.

The final tables provide some useful guidelines for audit committees when assessing their role and performance on fraud prevention and detection.

**How do you know if your oversight is effective?**

The best way is to ask some straightforward questions on your committee's activities:

1. Is adequate meeting time dedicated to the consideration of fraud?

2. Do you consider fraud when reviewing the financial statements, in particular the entity's significant accounting principles, policies, estimates, and non-routine transactions?

3. Do you evaluate management's assessment of risk?

4. Have you asked the independent and internal auditors as to their views on the potential for fraud, and how well management respond to the risk of fraud?

If you have these matters comfortably under control, then you are most likely to be effective in the role.

# The Audit Committee's Role in Business Continuity Management (BCM)

Whether from natural causes such as fires and floods, technical or human causes, or a combination of events, there are many possible scenarios that can bring organisations to an abrupt halt. Business continuity is about maintaining the uninterrupted availability of all key business resources required to support essential business activities. An organisation's business strategies and decisions are based on the assumption that the business will continue indefinitely.

An event that violates this assumption is a significant occurrence in the life of any organisation, directly impacting its ability to fulfil its business objectives.

**Who is responsible for BCM?**
While the prime responsibility for ensuring that organisations have proper business continuity planning rests with the board of directors and senior management, Audit Committees need to understand their own responsibilities in this area.

Increasingly, audit committees are expected to oversee risk management processes in order to ensure that financial reports clearly reflect an organisation's risks and exposures. Audit committees are required to understand how the risk management process is tailored to the company's specific needs, investigate whether the process is ongoing, ensure that the individuals responsible have appropriate stature, expertise and time, and meet periodically with the chief risk officer.

In addition, the audit committee needs to oversee the activities of the internal audit department, which is responsible for ensuring that all business processes and internal controls, including corporate governance and risk management processes, operate effectively and efficiently.

As a result, whether specifically referred to or not in the Audit Committee charter, BCM is an integral part of the risk management framework within an organisation. As such, it should be included in the audit committee's oversight responsibilities.

Increasingly, audit committees are expected to oversee risk management processes in order to ensure that financial reports clearly reflect an organisation's risks and exposures.

**So what is BCM?**
BCM is defined as the development of strategies, plans and actions which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to organisations.

The main components of the BCM process are:
- Crisis Management
- Crisis Communication
- Business Resumption Planning
- IT Disaster Recovery Planning.

Audit committees may find it difficult to assess whether the BCM process is adequate. Aspects that may provide some comfort include:
- Formal standardised policy and procedures, including IT disaster recovery plans; emergency response procedures; off-site storage of records; backup and recovery procedures; evacuation plans; communications strategies and media liaison strategies. Documented plans for different scenarios.
- Identified recovery locations and the existence of current hot-site contracts.
- Testing of plans including the maintenance of adequate documentation of testing results.
- Training materials and evidence that regular training (awareness and specific) has been conducted.
- Adequate budget allocation for BCM.
- Service level agreements with service providers for the provision of services in the event of a disaster.
- Evidence that regulatory requirements are taken into account in the policy and procedures for disaster recovery; that requirements for daily business continuity are included in the Operational, Health, Safety, Security and Environmental policy, procedures and processes, and that compliance is monitored.

The key components of an effective BCM are illustrated on the following page.

| People (65%) | Infrastructure (30%) | Plans (5%) |
|---|---|---|
| ▪ cohesive team<br>▪ chain of command<br>▪ proper nominations:<br>- ability<br>- authority<br>- specialists<br>▪ alternates<br>▪ clear roles<br>▪ trained personal<br>▪ awareness<br>▪ accountability | ▪ command centres<br>▪ business facilities:<br>- operations<br>- open offices<br>- private offices<br>- meeting rooms<br>- public areas<br>▪ furniture / fit out<br>▪ resources:<br>- equipment<br>- systems access<br>- communications<br>▪ vendor support | ▪ action driven<br>▪ simple / concise<br>▪ in-house WP tools<br>▪ checklists<br>- generic<br>- worst case<br>▪ terms of reference<br>▪ team information<br>- reference guides<br>- listings<br>- plans / diagrams<br>- contact numbers |

The audit committee can obtain comfort regarding the adequacy of BCM by:

- Continuous discussions with executive and operational management on how the BCM process is managed in the organisation.
- Discussions with the risk officer to establish how BCM is integrated with the organisation's risk management processes, and whether adequacy assessments have been made.
- Engaging industry specific BCM experts to perform independent evaluation and benchmarking exercises.
- Utilising internal audit to perform audits, including benchmarking, of the BCM process (providing internal audit has the necessary skills to do so).
- If appropriate, peer reviews could also provide valuable benchmarking information.

BCM consists of business process controls to ensure that the continuity of business operations is achieved.

**In conclusion:**
The long term objective of most organisations is sustainability. This will lead to the achievement of their long term goals and those of their stakeholders. Effective and adequate BCM provides assurance, albeit not absolute assurance, from a business continuity perspective that the organisation can survive a disaster. However, it cannot prevent business failure due to inappropriate business strategies or management decisions and actions.

BCM is included in the scope of the Audit Committee in three different ways:

- BCM is part of Enterprise Risk Management. Therefore an organisation should identify all the potential events that could impact it from achieving its objectives and develop and implement risk response to mitigate risk to prevent or minimise the impact.
- The oversight of an effective and efficient Internal Control Framework is an audit committee responsibility. BCM consists of business process controls to ensure that the continuity of business operations is achieved. With the occurrence of events that could impact business continuity, there are policies, procedures and controls that need to be exercised to ensure the impact of disruptions is limited.
- Internal audit should ensure all business processes and internal controls, including governance and risk management, are sufficiently effective and efficient to prevent business disruptions. The audit committee is responsible for reviewing and approving the scope of internal audit's review of BCM.

# PricewaterhouseCoopers' 9th Annual Global CEO Survey - Globalisation and Complexity

PricewaterhouseCoopers released the results of its 9th Annual Global CEO Survey in January 2006. The survey focuses on globalisation and complexity - two powerful and inevitable forces that are top of mind among the 1,400 CEOs who participated in this survey.

The survey was conducted in 45 countries throughout the world in the last quarter of 2005.

Some of the data challenges conventional thinking. While today's companies are expanding across the globe-especially into emergingmarkets like Brazil, Russia, India and China (BRICs) - they are doing so primarily to find new customers and to service existing one not to seek cost reductions. But globalisation and other factors create complexity that must be managed successfully when it adds value, or reduced when it does not.

In addition to these findings, this year's report features one-on-one interviews with five global business leaders. They bring in-depth, personal perspectives on how they and their organisations are meeting the challenges of globalisation and complexity.

The following is the summary of the survey,

**Support for globalisation is strong- and getting stronger.**
Over the next year, 58 percent of CEOs say that globalisation will have a somewhat or very positive impact on their organisations. However, when viewed over the
next three years, CEO confidence increases to 63 percent.

**Going global isn't easy.** CEOs cite overregulation as the chief challenge to globalisation (64 percent), followed closely by trade barriers / protectionism (63 percent), political instability (57 percent) and social issues (56 percent).

**Choosing among the emerging -** market countries, CEOs are investing the most resources in China (55 percent), followed by India and Brazil (36 and 33 percent, respectively) and then Russia (27 percent).

**Globalisation is no longer about cost cutting only.** CEOs say they are moving into the emerging-market countries like the BRICs primarily to find new customers and to service existing ones.

While CEOs see big opportunities in these emerging markets, going global creates complexity.

More than three-quarters of CEOs surveyed say the level of complexity in their organisation is higher than it was three years ago, and 27 percent say it is much higher. There's no end in sight though, as 41 percent of CEOs agree strongly that complexity is an inevitable by-product of doing business today.

**What creates the most complexity?**
Not surprisingly, expansion into new territories and mergers and acquisitions (both 65 percent) and launching new products and services (58 percent) are seen as the sources of the most complexity.

Still, CEOs say the advantages of these value-creating actions outweigh the disadvantages. For example, 88 percent of CEOs say that launching new products and services is a worthwhile initiative.

Nearly 80 percent of CEOs say they have made reducing unnecessary complexity a personal priority. Their primary focus areas: information technology (84 percent), organisational structure (79 percent), and financial reporting and controls and customer sales and service (both 69 percent).

One big problem, the findings suggest, is that there are significant gaps between the individual capabilities that CEOs view as important and their organisational performance in these areas. For example, significant capability gaps exist in the following areas: highly capable people (38 percentage points), effective communications (35 percentage points), and the ability to identify activities that are destroying value (31 percentage points) and creating value (26 percentage points)

Success breeds success; that is, performing well - with certain capabilities for managing complexity - correlates with performing well with others. CEOs who rate themselves as very good on measuring complexity (58 percent) or on having a corporate-wide framework (55 percent) have demonstrably higher ratings for each of the other capabilities than those who do not.

For audit committees, they should provide valuable insight in the challenges facing CEOs. This will enable audit committee members to understand the organisation's business strategies, to assess the risks and opportunities, and to evaluate the adequacy and effectiveness of risk responses and internal controls.

If you would like a hard copy of the survey, please contact Khun Tidayut Nophaket on 02 344 1352 or tidayut.nophaket@th.pwc.com.
This survey is also available on our global website www.pwc.com.

Your worlds  Our people*