The newsletter for Audit Committee members in Thailand

On Board*

Issue 3: June 2006

In this issue

p w c

*connectedthinking

Editors comments

Welcome to the 3rd edition of our quarterly newsletter for Audit Committees. Our first article is based on a recent **survey** and provides some revealing insights into the views of Audit Committee Chairman on the role and performance of internal audit. The business issues in this edition focus around **political risk** and **IT security** - two topics which, in our view, deserve greater prominence. The highlights are:

Survey results - Increased stakeholders' expectations and new regulations are driving changes in Audit Committee's responsibilities - long gone are the days when the Audit Committee had a narrow focus on financial reporting. With this in mind, Audit Committees need to make use of all available tools and techniques to ensure they execute their responsibilities as effectively as possible. One such "tool" is an effective internal audit function. It was therefore surprising to learn from a recent PwC survey that Audit Committee chairmen place low reliance on their internal audit function. **In this article**, we share with you the survey findings and how you can assess and improve internal audit's contribution in your organisation.

IT security - Information, from basic data to the strategically significant, is a key asset for all organisations. However, in our technological age, organisations are having to adjust and adapt to doing far more business using technology - to do this they need quality management information for themselves and their stakeholders. These demands require a new approach to ensuring that the information is protected. In our **second article** we explain why IT Security is important to the Audit Committee.

Political risk - We are all feeling the impact of increased globalisation whether from competition in domestic markets, or the challenge of expanding in new foreign markets. Many countries are also negotiating numerous Free Trade Agreements (FTAs). We are experiencing increased terrorist activity and are seeing the emergence of new political ideologies in a number of countries. All these factors are changing the way you need to assess and manage foreign investments. These so called "political risks" are now a significant part of decision making, risk management and investment management. Our **third article** provides you with insights on how political risk can be better understood and managed.

We trust you will find this edition helpful and we would also appreciate your feedback on how it might be improved by completing the enclosed feedback form and returning it to us.

Varunee Pridanonda
Partner

Recent events - IoD Audit Committee Roundtable June 1, 2006, JW Marriott Hotel, Bangkok

Working with the IoD, PwC recently hosted a roundtable discussion with audit committee chairmen.

What was the aim?
To help identify specific challenges facing audit committees in Thailand and how they might be addressed.

Who attended?
More than twenty audit committee chairmen from some of Thailand's largest corporates.

What was discussed?
The topics covered the audit committee's roles and responsibilities in respect of:

- Completeness, accuracy and reliability of financial reporting
- Enterprise Risk Management (ERM)
- Working with External Audit
- Working with Internal Audit; and
- Assessment of the audit committee and its individual members.

What happens next?

- PwC and the IoD will conduct a survey of audit committees and conduct interviews. The aim here is to further develop a viewpoint on best practices and solutions to common challenges in Thailand.
- The overall results will be distributed during a seminar for all audit committee members planned for later this year, and they will also be shared with regulators.
- If you would like to join the next roundtable discussion please let Khun Varunee Pridanonda know by contacting her on 02 344 1282 or at varunee.pridanonda@th.pwc.com

Getting the best out of internal audit – key findings from our UK survey of Audit Committee Chairmen

In January 2006, PricewaterhouseCoopers (PwC) conducted a series of detailed interviews with audit committee chairmen on the role and performance of internal audit. The survey covered 49 companies, predominantly from the FTSE 100 in London. The key findings were revealing:

On performance - More than one-third (37%) of chairmen indicated that internal audit delivered less than "very good" results. But meeting the demands of the audit committee means understanding and being clear about what those expectations comprise. The survey showed that, in fact, in very few cases can audit committee chairmen claim that they have made their expectations of internal audit clear.

On reliance - PwC was surprised to note that 38% of audit committee chairmen placed only low to moderate reliance on the internal audit function. Many reported that they looked far more to external audit, to their business sense, and to the track record of the executives. Here they reported feeling vulnerable, as they depended heavily on the quality of information that they received. They were very aware that operational management may not always be inclined to share bad news with them as quickly as they would like.

On skills - Audit committee chairmen felt that internal audit did not have the full picture, or the right skills, and in some cases the right remit to provide better assurance to them. We also found that the amount of reliance placed on internal audit was highly correlated to the clarity of expectations of the audit committee chairmen.

"The individual is too process focussed and does not pay enough attention to adding value."

On the premise that reliance will be related to trust and familiarity with the function, we asked about the regularity of meetings. Approximately half of those surveyed meet with the internal audit head six or fewer times per year. Many of them said that this was insufficient.

On reporting lines - A significant concern that emerged was that reporting lines threatened internal audit's role as an effective independent assurance function. Even with direct reporting to the Audit Committee Chairman, there was recognition that independence is threatened if he/she does not have an active involvement in the career path and reward of the Head of internal audit, as well as in the funding of the function. Some chairman went as far to say that a reporting relationship to the CFO was a "conflict of interest".

"It's a conflict of interest to report to the CFO as most the risk arises from the finance function itself."

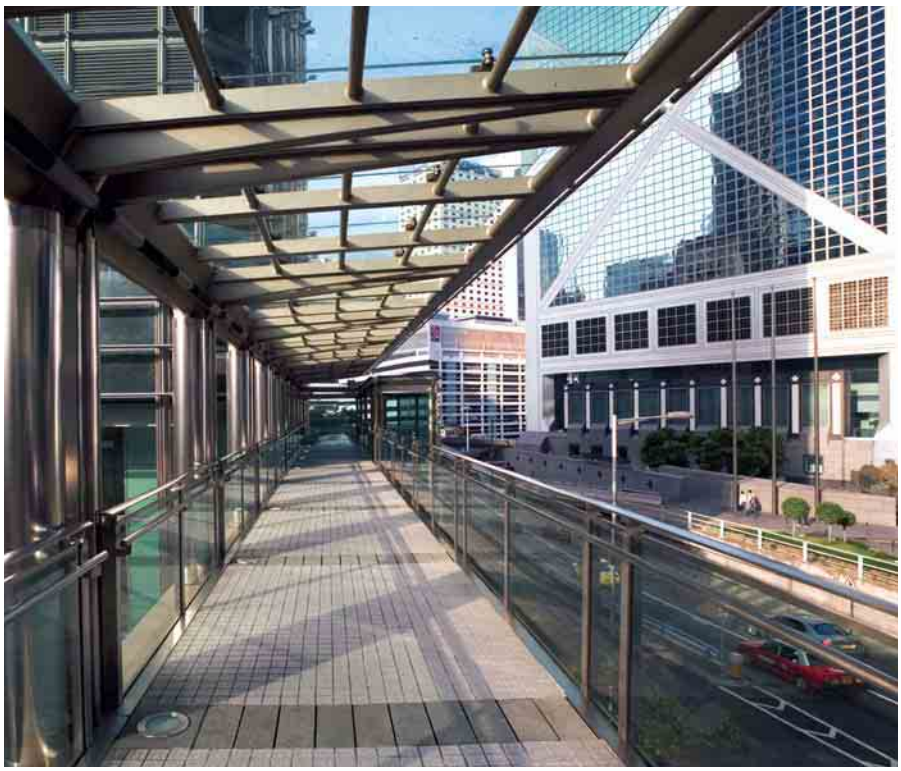
On reporting - In addition to the meetings that take place, reporting is a key part of the interaction between the audit committee and internal audit. Many (72%) chairmen reported that the quality and relevance of the reporting received was high or very high. However, 50% indicated that they received too much information. Many of these would prefer to see shorter and more focused papers.

"Often the really tricky issues or ones you can't prove get left because they can't be put in the report."

When probed further on the completeness of the reporting - specifically, "How do you know the reporting is complete?" - almost one-third responded that they did not know. One quarter said they relied on their relationship with the head of internal audit to give them comfort over completeness, whereas 19% relied on external auditors or executive management and 7% relied on their intuition.

On the way forward - Many audit committee chairmen want to see more operational and commercial experience in the internal audit role. But finding suitable candidates may prove tough. An alternative to external candidates would be to bring top-quality internal candidates through the function as part of their career development. It was noted that a number of organisations do this. Many, however, questioned whether their organisations had an appetite for this.

"We would like to have an Internal Audit function like GE, where high fliers must cycle through Internal Audit as part of their management training."



The challenges faced by Audit Committee members.

- They are not fully clear about their own expectations and as a result are not clearly driving the assurance agenda.
- They question the skills that their internal audit functions have to fulfil expanding expectations.
- They question the independence of functions that either report directly to, or are substantially controlled by, the finance director.
- They believe that the role of internal audit is being shaped by its capabilities and not by the business's need

So what should be done - how to break the impasse (all of which require the active participation of the audit committee chairman)

- They should be constantly challenging their internal audit head to increase the relevance of the work that internal audit does to critical issues on the audit committee's agenda.
- They should periodically ensure that the annual obligatory review of the effectiveness of internal audit is independent, and that its coverage is appropriate.
- When the head of internal audit changes, committee members must be actively engaged in recruiting the replacement.

In conclusion - internal audit needs to do better

From the survey results, it appears that internal audit has yet to gain the professional trust and reliance of UK audit committees. Perhaps influenced by the "lowly" role internal audit is perceived to have - a role propagated by low salaries and little inter-organisational influence - audit committee chairmen don't have a lot of positive things to say about the effectiveness of their internal audit functions.

How does an audit committee chairman assess whether he/she gets the best out of internal audit?

The Audit Committee chairman can obtain the services of an external service provider to perform a quality review of the internal audit function (in-house or outsourced). The Institute of Internal Auditors (IIA) Standard: 1312 on External Assessments requires external quality assurance reviews to be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organisation.

External reviewer qualifications include:

- Independent of the organisation and internal audit department, and
- Competent in the professional practice of internal auditing and the external assessment process.

The Audit Committee chairman should use this opportunity to expand the scope of the external assessment from compliance with IIA Standards to include best practice benchmarking, and an assessment of how well aligned internal audit is to business objectives and stakeholders' expectations - Strategic Internal Audit Function.

For more information on Quality Assurance Reviews, please send an e-mail to *varunee.pridanonda@th. pwc.com* or fax for her attention at *02 286 4440.*

Why does Information Security matter to the Audit Committee?

In today's global business environment, the significance of information is widely accepted, and information systems are truly pervasive throughout business and governmental organisations. The growing dependence of most organisations on their information systems, coupled with the risks, benefits and opportunities IT carries with it, have made IT governance an increasingly critical facet of overall governance. Boards and management alike need to ensure that IT is aligned with an enterprise's strategies, and that enterprise strategies take proper advantage of IT - from "IT Governance Institute - ITGI"

Many of the basic roles of IT have been around a long time and need little explanation. IT provides communication infrastructure, business applications, records repository, analytical decision support, and tracking and control mechanisms. Companies see IT as a field that can help them sustain their growth. The IT industry in the last five to ten years has moved from being predominantly hardware and software manufacturers to being predominantly service providers.

A newer, emerging role of IT is recognition that a robust information support structure is a critical component of enterprise governance. More than ever, clear, accessible information is vital to boards and senior executives. Accurate and reliable information, both internal as well as external, is critical to decision making.

What is Information Security?
Security relates to the protection of valuable assets against loss, misuse, disclosure or damage. The information must be protected from vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage. Protection arises from a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls. These safeguards should address both threats and vulnerabilities in a balanced manner.

The objective of information security is "protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity". While emerging definitions are adding concepts like information usefulness and possession. The security objective is met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from failures (availability)
- Information is observed by or disclosed to only those who have a right to know (confidentiality)
- Information is protected against unauthorised modification (integrity)
- Business transactions as well as information exchanges between enterprise locations or with partners can be trusted (authenticity and non-repudiation)

Who should be concerned with Information Security Governance?
Mostly information security has been dealt with as a technology issue only, with little consideration given to enterprise priorities and requirements. Responsibility for governing and managing the improvement of security has consequently been limited to operational and technical managers.

However, for information security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required. For information security to be properly implemented, skilled resources such as information systems auditors, security professionals and technology providers need to be utilised. All interested parties should be involved in the process.

Boards and management have several fundamental responsibilities to ensure that information security governance is in force. They should at least:

- Understand why information security needs to be governed
- Ensure it fits in the IT governance framework

Effective security is not just a technology problem, it is a business issue. Related risk management must address the corporate culture, management's security consciousness and actions. Sharing of information with those responsible for governance is critical to success.

How can security risks be managed?
An information security programme is a risk mitigation method like other control and governance actions and should therefore clearly fit into overall enterprise governance. IT governance itself is emerging as a subject matter and integral part of enterprise governance, with the goal of ascertaining that:

- IT is aligned with the business, enables the achievement of business goals and maximises benefits,
- IT resources are used responsibly, and
- IT related risks are managed appropriately.

Within IT governance, information security governance becomes a focused activity, with specific value drivers: integrity of information, continuity of services and protection of information assets.

Hence, information security should become an important and integral part of IT governance. Negligence in this regard will render the creation of IT value unsustainable in the long run.

What is the Audit Committee's role in IT Security and IT Governance?
The roles and responsibilities of the Audit Committee is determined by the Board of Directors or specific regulations, and is likely to cover IT Security and IT Governance. Furthermore, the Stock Exchange of Thailand's Best Practice Guidelines for Audit Committees require them to review the adequacy and effectiveness of internal control systems and internal audit functions by coordinating with the external auditors and internal auditors. Internal control systems include governance, risk management and business control processes, including information technology. Internal audit can provide the audit committee members with valuable assistance by giving objective assurance on these processes, including IT.

References

- IT Governance Institute, *Information Security Governance Guidance for Board of Directors and Executive Management, COBIT (Control Objectives for Information and related Technology) 3rd Edition, 2000, www.ITgovernance.org and www.isaca.org,*
- International Organisation for Standardisation, *Standard 17799, 2000*
- British Standards Institution, *BS 7799-2—Code of Practice for Information Security Management,* 1999

How managing political risk improves global business performance*

Companies are drawn to expand into international markets in search of lower costs, new opportunities, and access to resources. When they arrive, however, they often find that the politics of foreign environments adds risk and complexity to business performance. A question for companies operating internationally thus becomes how best to manage political risk.

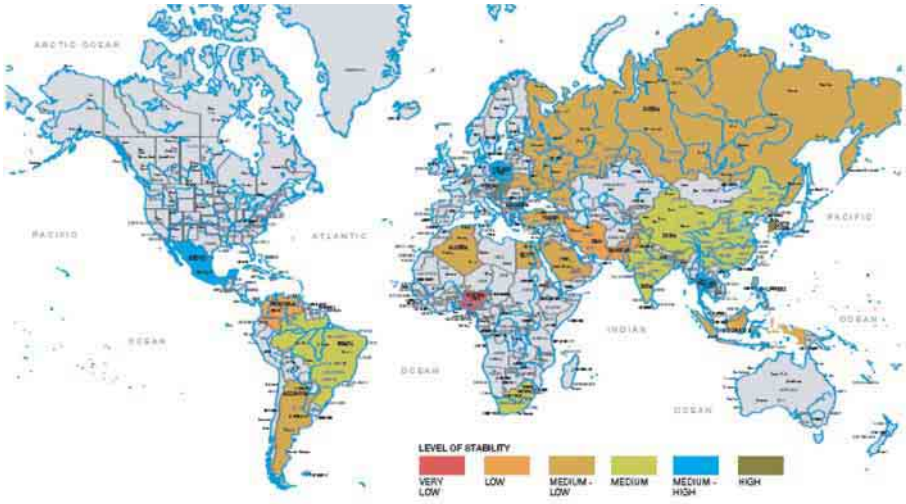
Political Risk: Any political change that alters the expected outcome and value of a given economic action by changing the probability of achieving business objectives.

Multinational companies as a group are making efforts to manage political risk, but most are not as effective at this as they think they should be. In a recent PricewaterhouseCoopers and Eurasia Group study, the vast majority (83%) of respondents said they engaged in ongoing monitoring of the political environment after an investment had been made, but nearly as many (73%) did not feel that they had effective political risk management processes. Risk managers, chief financial officers, and international division heads contacted for our survey said frequently that the complex web of information that would enable them to assess political risk was difficult to obtain and evaluate. Many expressed frustration that when they were able to glean information from local sources, the information was inevitably biased. Moreover, funding for specific risk management techniques (e.g., risk mapping) was often lacking within their organizations, because the benefits were not well understood.

As a result, CEOs and boards of directors were not receiving the timely, accurate information they needed to make effective decisions about international exposures—or, conversely, information was not effectively communicated and utilized to manage risk in the field.

Executives of global companies are clearly challenged regarding how best to assess political risk, factor it into their investment decisions, and use the knowledge to help improve global business performance.

Asia region has a low level of political stability and is deemed to have a higher political risk factor



By their nature, emerging markets are places where political decisions have a greater effect on markets than economic trends, thus diminishing the value of employing economic guideposts to investment decisions. In politics, risks are more difficult to identify, to measure, and to hedge. Consequently, investors ranging from hedge funds to extractive industries are extremely concerned with the risks of nationalisation, weak legal systems, corruption, and regulatory stability. Corporations exposed to these risks must weigh, as an example, the trade-offs associated with investing in China versus Brazil or Germany versus Japan.

"We have to be and do business in China what ever it takes" AND "Our political risk, being an Asian company, is lower than our Western counterparts"

There are two emerging political risk philosophies developing:

1. It seems that Corporations are treating China as an exception to any of their established political risk policies. World-wide corporations see it as a strategic priority to do business in China irrespective of the political risks involved. The driver for this desire is not only because of the size of the potential market, but a corporation without a business venture in China is perceived not to have a global footprint.

2. There is a belief with Asian corporations that being from Asia reduces their political risk in the region. Although Asian countries' cultures differ significantly, Asians do associate themselves better with eastern culture, and potentially trust this culture more than western culture.

We do not challenge the validity of these philosophies but believe that corporations doing business in or with some of the world's fastest-growing economies, especially China and India, or more risky economies require a framework for navigating the challenges associated with working in these countries, which typically have rapidly evolving political and legal frameworks. This framework will include setting the risk appetite for each country, risk tolerance levels and potential exit strategies.

"Political risk is outside our control and we cannot do anything about it"

Experience tells us that there are two fundamental ways in which managing political risk improves global business performance:

1. Protecting new and existing global investments and operations by helping management anticipate the business risk implications of political change or instability.

Prepared and aware, management is more likely to be able to exit markets that are in danger of becoming too unstable. Where short-term instability does not dampen the appetite to pursue long-term opportunity, management can implement risk mitigation and operational oversight to control against shocks.

2. Capitalizing on opportunities resulting from political change. For a company constantly on the lookout for new opportunities, monitoring political risk within target regions or across continents can help management hone in on political developments that foretell a business boom, beating competitors to the punch.

By establishing a systematic approach to political risk management, multinational companies can drive business performance improvement. We know that the task of managing political risk is not easy. Not only do political changes pose direct risks to firms, but politics is also a component of other external risks. Regulatory changes have the potential to promote or inhibit market competition, social risks often have political bases and responses, and political mismanagement can turn natural or human-made events into catastrophes. Moreover, political risk is often perceived to be outside of management's control, making it difficult to define, predict, and align with objectives. Given the complexityof these issues, it is no wonder that corporations often fail to address political risk in a systematic way.

PricewaterhouseCoopers and Eurasia Group believe that political risk can be managed effectively. We believe that doing so requires integrating political risk management into a systematic process embedded in a company's business processes, and characterized by the same principles or components that apply to effective enterprise risk management. The underlying principles of the systematic political risk management process we advise are:

1. **Political risk management starts at the top**
   Senior management needs to be mindful that politics is a driver that creates both risk and opportunity. Executives must accept responsibility for managing political risk, set guidelines for approaching it comprehensively, and factor political risk assessments into decision making about global strategy and ongoing operations.

2. **Managing political risk directly impacts performance**
   Most companies manage political risk in order to avoid financial surprises, but effective risk management can also enable companies to capture opportunities they may not otherwise have seen. Indeed, while corporate leaders are often acutely aware of the potential downside risks of international investments, changes to the political, social, and economic environment can also produce windfalls.

3. **Evaluating political risk optimizes decision making**
   In addition to return on investment, management should also consider political and other types of risk when making capital allocation and strategic and operational decisions. This improves alignment with corporate objectives and risk appetite, yielding better decisions. When making performance-related decisions, management should also consider its portfolio of political risk.

4. **Assessing risks before taking action delivers value**
   Companies need a comprehensive framework for identifying and assessing all of the risks they face, understanding interdependencies, and assessing the impact of risk. Such a framework enables development of mitigation strategies that support company operations through crisis and change. The formal process of gathering and assessing data on political developments should be overseen by a risk manager and disseminated at the corporate, operating unit, and regional level.

5. **Systematic political risk management protects investments**
   Management should evaluate and manage political risk when making investment decisions, and then continue monitoring such risk routinely in support of ongoing operations. Most companies do not do this today. Sixty-nine percent of the companies we surveyed incorporate a measure of political risk into their financial projections for new investments. Yet once operations are established, those same companies are less focused on ongoing monitoring of political risk, with only 27% of our respondents producing formal reports two or more times a year.

   After market entry, companies must monitor political risk on an ongoing basis and use this information proactively to inform investment, operating, and divestment decisions. Hence, it is essential that management of political risk be embedded into operating business processes, in order to protect investments.

Communication of risks and their business impacts is a central component of embedding political risk management into operating processes. Inadequate communication networks, combined with decentralized organizational structures, often prevent companies from using risk information effectively in operational decision making. As a result, decision making fails to adequately weigh the risks, leaving investments increasingly exposed over time.

Companies may want to formally assess their current political risk management process to determine how well it adheres to the structured principles we have outlined here. This assessment can be undertaken with the following steps:

1. Map the politics
2. Evaluate the risks
3. Assess controls and plans
4. Determine the acceptability of residual risk

Integrating Political Risk into an Enterprise Risk Management Process
COSO's Enterprise Risk Management (ERM) Framework provides a comprehensive approach to helping businesses and other entities assess and enhance their internal control systems. Political risk represents an indispensable part of this larger puzzle. Political risks are part of the external risks that need to be identified as companies assess their as-is environment, and global strategies should be designed to maximise trade-offs in investment-location decisions and continuously monitor the political environment.

In conclusion
Political risk is one of the risk categories that need to be assessed when corporations perform their assessment of all the business risks impacting the achievement of their objectives. It should be managed as part of the ERM framework. In some corporations, the Audit Committee has been delegated (by the Board or per regulations) the responsibility to ensure the ERM framework, policies and procedures are effective in identifying and managing risks impacting the organisation.

"What is your responsibility for ERM and does your organisation consider political risk?"

You can read more about PwC and Eurasia Group, our view on political risk and services we offer by visiting our website http://www.pwc.com/extweb/pwcpublications.nsf/ or contacting Khun Varunee Pridanonda or Marius Kunneke on 02 344 1000, extension 1282 or 1025, respectively.

Your worlds  Our people*