



AUDIT COMMITTEE INSTITUTE

Audit Committee Insights International
2007 Annual Digest

KPMG INTERNATIONAL



Contents

Welcome

Regulations

- 2 Fiscal (Audit) Committee Played Big Part in Sarbanes-Oxley Compliance at Brazilian Firm
- 4 What the UK's New Companies Act Means for Directors' Duties
- 7 As South African Rules Change, Emphasis Is on Audit Committee Independence

Duties and Responsibilities

- 10 'Joined-Up' Approach Works for Irish Audit Committees, Management
- 13 Prevent, Detect, Respond: Taking Corruption Seriously
- 16 Corporate Governance Convergence Is a Global Problem

Risk Management

- 18 What ERM Means for Corporate India
- 22 Audit Committees: Decide on Who Does What in Risk Management

Financial Reporting and Internal Controls

- 25 Sustaining Financial Controls That Contribute to Business
- 29 Making the Control Environment Relevant in a New Regulatory World
- 34 French Audit Committees Smooth the Transition to IFRS

Information Technology

- 36 For Brazil's Audit Committees, IT Governance Is Here to Stay
- 39 How To Make IT Governance Work for Audit Committees
- 42 As Technology Committees Grow, Audit Committees Lend a Hand

Register for KPMG's Audit Committee Insights

KPMG LLP (U.S.) distributes a biweekly electronic publication to help audit committee members, executives, and others stay up to date on the ever-increasing volume of news, opinions, research, and trends related to corporate governance and the role of the audit committee. KPMG's *Audit Committee Insights* contains relevant articles selected from hundreds of sources on such topics as financial reporting, audit committee surveys, and shareholder issues. It also features articles offering KPMG's commentary, perspectives, and insights on key issues leveraging the knowledge gained through KPMG's Audit Committee Institute. Registration for this complimentary electronic publication is available at www.kpmginsights.com.



Welcome to the *Audit Committee Insights International* 2007 Annual Digest

The quality of the insights that members of the audit committee (or equivalent supervisory committee), directors, and senior management bring to their boardroom discussions can have a tremendous effect on the quality of the oversight process. However subtle they may be, such insights can be pivotal to achieving the transparency, integrity, and sound governance that stakeholders expect.

Embarking on our second year of publishing the electronic biweekly journal *Audit Committee Insights International*, we continue to explore the critical factors underlying the effectiveness of audit committees. This *2007 Audit Committee Insights International Annual Digest* offers a collection of *Insights* articles focused on issues and practices shaping audit committee agendas around the world—from the sharpening focus on oversight of risk management to evolving practices in audit committee self-assessments and oversight of auditors.

It is evident from readers' feedback—and by our growing readership of nearly 18,000, including *U.S. Insights*—that *Insights* has come to play an important role in supporting audit committee oversight processes. We consider our commentaries to be part of an ongoing, international dialogue among audit committee members, directors, management, auditors, and others with a role in financial reporting and audit committee governance.

We hope you find this annual digest helpful in your efforts to support the audit committee and strengthen the financial reporting process. If these and other *Insights International* articles trigger new thinking, prompt pivotal questions, or otherwise elevate the quality of the dialogue, then we are accomplishing our objective.

KPMG's Audit Committee Institute

***Audit Committee Insights International* articles are supported by research from Audit Committee Institutes of KPMG member firms around the world, and include analysis from KPMG professionals as well as commentary on leading practices from prominent audit committee chairs, directors, executives, and corporate governance observers.**



Regulations

Fiscal (Audit) Committee Played Big Part in Sarbanes-Oxley Compliance at Brazilian Firm

When Brasil Telecom needed to become compliant with the Sarbanes Oxley Act in the United States, the telecommunications provider took the necessary steps to achieve compliance, which included setting up a special committee that worked with the fiscal, or audit, committee.

The telecommunications firm has been listed on the New York Stock Exchange since 1998, making it subject to American securities law – and S-O compliance.

Brasil Telecom S.A. provides local, intra-regional long distance, network, data communication and other value-added services to more than 40 million people throughout Brazil.

Joao Carlos Orzzi Lucas, director of internal audit at Brasil Telecom, spoke with Audit Committee Insights International about his company's greatest challenges in complying with S-O.

Audit Committee Insights International: What preparation was needed to make the transition to S-O compliance?

Lucas: At Brasil Telecom, we identified the principal company operations, as elaborated in our financial statements. We then identified the related system applications that supported these operations to evaluate the risks and necessary controls.

Naturally, we consulted management first to confirm that our evaluation was correct, and then we began tests of effectiveness and security. We created a special Department for Risk Management, which worked in conjunction with internal audit to give greater adaptability to the preventive model of risk management and control.

ACII: What roles did the internal committees play in this preparation?

Lucas: The Supervisory Board played the fundamental role of sponsoring the process, giving the necessary powers to the appropriate channels and arranging the distribution of tasks between actors where necessary.

To give greater adaptability and [help] ensure correct follow-up, a committee called the "SOX committee" was created, which included the principal executives of the company. This committee worked closely with the fiscal committee (a special Brazilian entity that closely resembles the audit committee, and which has been accepted by the U.S. Securities and Exchange Commission as an equivalent) along with the internal audit and the risk management departments.

This group met every week to report on the progress of the effectiveness and security tests for the migration. Each week the group considered possible challenges and found ways to resolve them.

ACII: Was a great deal of communication with management necessary?

Lucas: Given the vast number of processes and controls that had to be tested and managed, as much for internal audit as for the external auditors, it was necessary to have regular and broad contact with management. Managers indicated the focal points at which we directed our attention.

A motivational and public relations campaign was undertaken within the company on the importance of internal controls, and the correct way of using them.

ACII: What were the greatest obstacles to the transition?

Lucas: As in any large company, Brasil Telecom uses a vast number of system processes that demand a considerable effort at documenting, updating and monitoring. This was especially difficult because, at the time, our company did not have a computerized risk management system.

As the most important controls required by S-O were computer-based, most of our efforts were dedicated to putting the information system into shape to deal with the new requirements. This also required a considerable investment in both computerized and manual controls. A large number of training sessions for our professionals was also necessary, especially during the last months of the year to [help] ensure that the job of S-O compliance had been completed.

ACII: How would you describe the results of your S-O compliance initiative?

Lucas: We achieved a great step forward in terms of corporate transparency and in risk management. When we finished, we also had a much better sense of our corporate processes, as well as how to give management a more responsible role in maintaining reliable information delivery.

These processes and controls are now integrated into our daily work. We were not prepared for the amount of change when we drafted our plans for the move to S-O compliance.

“The Supervisory Board played the fundamental role of sponsoring the process [of making the transition to Sarbanes-Oxley compliance].”
—Joao Carlos Orzzi Lucas,
director of internal audit at
Brasil Telecom

Originally published August 29, 2007.



Regulations

What the UK's New Companies Act Means for Directors' Duties

By Sarah Ray, Senior Manager, KPMG's UK Audit Committee Institute, and Andrew Rosenbaum, Contributing Editor, *Audit Committee Insights International*

The codification of directors' duties under the new Companies Act of 2006 (CA) in the United Kingdom may pose challenges for audit committees, as government agencies try to put corporate social responsibility onto the boardroom agenda.

The law, which passed in November 2006, is the first time directors' general obligations have been made law after centuries of being included in case law only.

"Many fear that the codification of directors' duties will create new problems rather than creating greater certainty," says Will Chalk, corporate legal director at the law firm of Addleshaw Goddard.

"The primary concern is that it moves away from the long-standing, overarching principle of acting in the best interests of the company, not least by requiring directors to consider the long-term consequences of any decision and the interests of a range of different and potentially competing interest groups," Chalk says.

Previously, directors' general duties were contained in a broad body of case law developed over centuries. Consequently, the CA aims to make the law regarding directors more accessible.

The law requires directors to act within their powers; exercise independent judgment; exercise reasonable care, skill and diligence; not accept third-party benefits; avoid conflicts of interest; declare interests in proposed company transactions; and promote the success of the company for the benefit of its members as a whole.

CA 2006 also was designed to be an aid to corporate administration.

"The deregulatory elements of the CA 2006 will simplify considerably the administration of companies, particularly private companies," Chalk says. "This is good news for listed companies with large group structures as well."

But it may not be such good news for audit committees, says Davida Marston, who is a member of the audit committee at ACE European Group, Europe Arab Bank and CIT Bank. Marston also chairs the audit and risk committee for Midland Heart, the largest housing group in the Midlands (UK). She thinks the CA could make administration more complicated.

"[CA 2006] merely regulates a way of decision making, which was already present," Marston says. "But this process, which was already in place, may now require a more structured recording and monitoring administration."

"The primary responsibility for [considering the impact of decisions] rests with the board and it is then the audit committee's job to monitor the structure (controls) established to ensure that the wider obligations are being considered as with any other procedure or control," Marston says.

During KPMG's ACI UK technical update seminars held in December 2006, the new directors' duty of promoting the success of the company was highlighted as a particularly problematic area. The duty requires directors to consider a non-exhaustive list of factors, including the likely consequences of their decisions in the long term and their impact on the company's employees, community and environment.

If the ACI seminars are a gauge of the reaction of directors across the country, this duty poses a number of questions:

- What is "success?"
- Is success the same as acting in the best interests of shareholders?
- Will boards have to demonstrate that success in regard to these potentially competing factors when making decisions and, if so, how should they go about doing so?

Marston says that this will affect the way in which decisions are made.

"It will require boards to ensure that when considering or approving the strategic direction of the business and individual business decisions that there is a documented process demonstrating that they have considered the implications," Marston says.

"It is that trail that audit committees will need to monitor. Thought will be required on the format of the linkage between the main board decisions and audit committee oversight requirements."

Chalk believes companies will need to decide how to reflect the new requirements when making and documenting decisions, despite the Attorney General Lord Goldsmith stating that there should be no need for an additional "paper trail."

Marston does not think that it will be more difficult to make business decisions.

"From a practical business decision standpoint, I don't think much should have changed as boards would have been remiss if they had not given serious consideration to the broader consequences," she says. "Even where something may have a negative impact on a particular aspect – i.e. the need for redundancies – this does not mean that it will not get done."

"Many fear that the codification of directors' duties will create new problems rather than creating greater certainty."

—Will Chalk, corporate legal director, Addleshaw Goddard

“Thought will be required on the format of the linkage between the main board decisions and audit committee oversight requirements.”

— Davida Marston, audit committee member of ACE European Group, Europe Arab Bank, and CIT Bank

Boards will need to demonstrate they have established a fair process and treated the workforce with sensitivity, Marston says.

“Similarly with the greater liability for environmental damage, any company with potential risk area should already have it recorded in the risk register with controls established to ensure appropriate consideration and all other important aspects such as the need to consult and communicate appropriately,” she says.

The UK government’s Department of Business, Enterprise and Regulatory Reform (formerly the Department of Trade and Industry) has issued guidance that, according to Chalk, states that “as long as the factors attendant to any decision are considered in deliberations, the overriding duty of directors is to promote the success of the company and, for a normal commercial company, this means to strive for a long-term increase in value.”

Many larger companies with particular sensitivities would already have a dedicated risk committee that would ensure that the risks arising from key strategic decisions were recorded in their risk register, Marston says.

For Marston, the codification of directors’ duties may require only a slight shift in the operation of a well-run board.

This effect might not be borne out until the courts make the full meaning of the law clear.

“Unfortunately, only time and a body of expensive case law will tell how the courts interpret and apply the new legislation and whether these provisions constitute, as some have suggested, an activists’ charter,” Chalk says. “It is hoped that the courts will maintain their robust reluctance to second guess the good faith business judgements of directors but, at the moment, we just don’t know.”

Andrew Rosenbaum is a London-based journalist who writes frequently on business and finance.

Originally published July 18, 2007.

Regulations

As South African Rules Change, Emphasis Is on Audit Committee Independence

By Gary Larkin, Managing Editor, *Audit Committee Insights International*

As many South African public companies cope with an impending shortage of financially literate, independent audit committee members, there may be a solution.

Industry observers are calling for the integration of audit committee education with the self-evaluation process, as companies prepare to meet stricter corporate governance requirements. This type of education would focus more on a company's business strategy and less on new and revised corporate governance rules.

Those rules include the Corporate Laws Amendment Bill (CLAB), a proposal that sets rules for audit committees, and the Auditing Profession Act, which regulates the external auditors serving public interest companies.

The integration of education and self-evaluation is necessary, according to Mervyn King, who headed South Africa's King Committee on Corporate Governance in 2002 and is now an audit committee chairman for furniture retailer Joshua Doore. King says integration can help stave off a possible shortage of informed, non-executive directors; the proposed CLAB mandates more such directors.

Audit committee members and external auditors are worried companies will meet the letter of the law but miss the spirit of the new corporate governance measures.

And considering that the Johannesburg Stock Exchange has 685 listed companies with 1,400 audit committee openings, it's clear why some companies are reluctant to raise standards when it comes to recruiting new audit committee members.

"Unfortunately, I believe the result will be that the size of audit committees in South Africa will decrease, due to the requirement that all members have to be non-executive members who act independently," says Lindie Engelbrecht, a director who works for KPMG's Audit Committee Forum in cooperation with the Institute of Directors (IoD), a South African corporate governance organization that helps set leading practices and provides board education.

"The minimum allowable number of audit committee members is two," she says. "And due to the shortage of experienced directors, I believe that some public interest companies will have to be satisfied with two members only."

Len Konar, an IoD board member and audit committee member for the World Bank, says prospective members must conduct good due diligence before deciding to join a particular audit committee.



**“Unfortunately, I believe the result will be that the size of audit committees in South Africa will decrease.”
—Lindie Engelbrecht,
director with KPMG’s Audit
Committee Forum**

“With the legislation on track, I would advise that there would be more circumspection before audit committee members consider joining boards,” Konar says. “What will happen in the future is that there [will] be directors who would accept fewer board appointments. They would be more selective.”

CLAB is before the South African parliament, while the Auditing Profession Act went into effect on April 1. The CLAB calls for public interest companies to establish audit committees and regulate their functions and composition, and the Auditing Profession Act affects the relationship between the audit committee and external auditors.

The CLAB states that all public interest companies must have at least two non-executive members who must act independently. The bill also requires audit committees pre-approve any proposed contract for non-audit services provided by the external auditor to the company.

In addition to creating a regulatory body to oversee and provide education and training for registered external auditors, the Auditing Profession Act places the auditor in position of whistleblower. That solidifies the auditor’s relationship with the audit committee, which already is responsible for the external auditor.

King takes issue with the proposal that all audit committee members are non-executive directors who act independently. He thinks the requirement doesn’t go far enough.

“We have to accept as common law that all audit committees have to be independent; the fact they can breathe makes them so,” according to King, who also sits on the audit committee of Luxembourg-based merchant bank and private equity investment house Brait SA.

He thinks audit committees should be made up of at least three members, with at least one being a chartered accountant.

“I don’t have to tell you the problems [with finding adequate] audit committee members in the U.S. under Sarbanes-Oxley,” King says. “[American] companies are taking a lot of our chartered accountants.”

King says that experienced directors should take new directors under their wing, in order to give them first-hand company knowledge. “Two to three years of that, and you will develop a pool of informed, non-executive directors who act independently in South Africa,” he says.

The importance of an education program for audit committees is twofold: to teach directors about the new and revised corporate governance rules, and to learn as much as they can about the company they serve.

“Boards should establish governance training programs for new and existing audit committee members to help ensure that all members are aware of their revised statutory obligations,” says KPMG’s Engelbrecht. “Other relevant topics should be included in these types of programs, including International Financial Reporting Standards, legislation and broad governance.”

At Brait, the audit committee has developed an 11-page self-assessment guide to rate its progress. The guide, based on eight categories of principles and practices, looks at how the committee handles financial statements, risk and control compliance and interaction with management and auditors. It also asks members for their opinions on committee composition, training and resources, the charter, meetings and how the committee deals with emerging issues.

Specifically, the guide asks for an effectiveness rating and follow-up steps taken regarding such issues as how well the committee scrutinizes management’s critical accounting policies, judgments and estimates. The guide also deals with the issue of the internal and external auditors’ assessment of internal control effectiveness.

While companies like Brait may be ahead of the curve, its self-assessment guide cannot be used to enforce corporate governance measures. Rather, it is a tool used for the audit committee to improve its oversight effectiveness.

“The whole international [trend] is to move away from criminal prosecution and move toward civil remedies,” King says. “At the moment, there must be 50 percent of [South African] companies that wouldn’t comply [with the Corporate Laws Amendment Bill].”

South African companies and corporate governance observers like King and others involved with the Institute of Directors don’t want to see a repeat of the corporate failures of the late 1990s.

“Finance Minister Trevor Manuel is on record in his 2002 budget speech as alleging areas of weakness in South African corporate governance,” Engelbrecht says. “While mentioning weak or non-existent governance structures, fiduciary irresponsibility of directors and negligent and sometimes reckless management, he placed emphasis on concerns over independence of auditors.”

And once the CLAB is in place, that oversight responsibility will belong to the audit committee.

**“We have to accept as common law that all audit committees have to be independent; the fact they can breathe makes them so.”
—Mervyn King, audit committee chair and head of South Africa’s King Commission on Corporate Governance**

Originally published August 2, 2006.



Duties and Responsibilities

'Joined-Up' Approach Works for Irish Audit Committees, Management

Ireland, with a population of just 5 million and a highly educated workforce, has become a magnet for foreign direct investment, registering annual growth between 5 and 10 percent over the past decade.

But with changes in the Irish Companies Act of 2003 and the UK Combined Code, as well as the introduction of the U.S. Sarbanes-Oxley Act following the wave of fraud, management and audit committees had to adapt. More importantly, Irish audit committees have had to strike a balance between meeting the regulations and keeping Ireland attractive to those foreign investors.

Kieran McGowan, a non-executive director and audit committee member for several Irish companies, including the international building materials firm CRH plc and Irish Life & Permanent, has been part of Irish corporate governance for many years. In addition to his experience with companies like CRH, McGowan has been plugged into governmental agencies that promoted business.

He was chief executive of Ireland's Industrial Development Authority from 1990 through 1998. McGowan was also chairman and president of the Irish Management Institute; a founding member of InterTradelreland, a domestic business development organization that promotes trade; and commissioner general for Ireland in relation to EXPO 2000 in Germany.

Audit Committee Insights International recently spoke with McGowan recently about Irish corporate governance matters.

ACI International: What are the top corporate governance issues in Ireland?

Kieran McGowan: There are four current top issues for audit committees. One issue is the documentation requirements of Sarbanes-Oxley (S-O) and the Combined Code.

Then there is the reconciliation of domestic GAAP financial statements to U.S. GAAP financial statements to International Financial Reporting Standards (IFRS), which is actually taking up a lot of audit committees' time.

Another area that comes to mind is the oversight of treatment of areas of judgment, such as revenue recognition and inventory valuation, in the preparation of financial statements.

Lastly, a number of the companies that [I serve] have been putting more and more time into oversight of the preparation of risk registers [inventory]. That is to ensure the risks are properly identified, along with the appropriate controls and ensuring that the process is dynamic. For example, that the register is a live document that is revisited by top management on a regular basis and not just a box ticking exercise.

ACII: What's your advice for any directors thinking about serving on an audit committee in Ireland?

McGowan: They need to give it plenty of time. I know from my experience that serving as an audit committee member can be as much as double the amount of time you need to serve as a director. At one of the companies, there are 10 audit committee meetings a year. Then [the full] boards have their own meetings.

Serving on an audit committee is really a great way to get a feel for the company. In dealing with financial reporting issues, you're also meeting with the finance director. You're boring in on issues.

ACII: How has serving on an audit committee in Ireland changed over the past six years?

McGowan: The number of meetings has increased. For example, we are now looking at trading updates [earnings forecasts]. It is a report to the market on the [company's] up-to-date trading position, which is issued a number of weeks before the financial statements themselves. The market now expects a heads-up some time before the end of the period.

ACII: What are the consequences of the changes in corporate governance regulations, such as the Companies Act 2003 in Ireland, the UK Combined Code and the U.S. Sarbanes-Oxley Act?

McGowan: It is getting tougher to find non-executive directors because of all the work involved. While the Combined Code calls for the rotation of directors, it is already hard enough to find new directors.

The secondary impact of the new regulations encompasses more documentation. For example, companies are now required to document specific intercompany [between parent companies and subsidiaries] trading relationships, intercompany pricing and other matters that up to now may have operated on a more informal basis.

ACII: As an audit committee member of construction materials maker CRH, how do you work with a company in which 90 percent of its sales, employees and offices are outside Ireland?

McGowan: In addition to normal processes, the audit committee – along with the rest of the board – takes the additional step on the issues. The audit committee visits the U.S. and Europe plants.

For a week at a time, we meet the management and the internal audit teams in Atlanta, Ga., and Amsterdam. We make sure the external auditors have the international breadth and reach to cover the countries we operate in. In the small number of cases where this might not be possible, we ensure a satisfactory working relationship with the relevant auditor; for example, in joint ventures.

“One issue is the documentation requirements of Sarbanes-Oxley (S-O) and the Combined Code.”

**—Kieran McGowan,
nonexecutive director, audit
committee chair for several
Irish companies**

“I know from my experience that serving as an audit committee member can be as much as double the amount of time you need to serve as a director.”
—Kieran McGowan, nonexecutive director, audit committee chair for several Irish companies

ACII: In regard to Ireland’s size, what are the challenges for Irish-based companies to build themselves into world-class entities?

McGowan: Traditionally, 30 to 40 years ago Ireland had a small industrial base. In the last seven or eight years, it has become a high-wage, high-cost economy. The basis by which Ireland competed before, which was as a low-wage, low-cost economy doesn’t exist anymore. It is now a knowledge-based, research-oriented economy.

ACII: Has there been much outsourcing?

McGowan: In the traditional sectors such as software/computer manufacturing, there are a lot of jobs being outsourced to Morocco, Poland, Czech Republic and India. Despite the outsourcing, we are at full employment and the gross domestic product was up 4.6 percent in 2005.

ACII: As the former chief executive of the Industrial Development Authority, what are the keys to maintaining proper regulation without losing direct foreign investment?

McGowan: First of all, regulations should be applied consistently. It should be principles-based, not full of nitty-gritty rules. Ireland has also adopted the Anglo-Saxon [corporate governance] model. That brought forth the Combined Code.

We try to have a “joined-up” approach to attract foreign direct investment. Because it’s a small place and we know each other, there’s a “joined-up approach” to regulatory [matters]. Instead of having some government department making an independent decision to build a road, that decision would be joined-up with a decision to build a business park, or third-level college or broadband inter-connectivity so that many aspects of planning and development are on the same page.

ACII: What does the future hold for Ireland Inc., and how much do corporate governance regulations play a part in that future?

McGowan: Since we are a small economy, we are affected by oil prices and exchange rates. And with pretty well full employment, the economy has transformed. We want to avoid overregulation.

ACII: What about the prevention of fraud?

McGowan: We’re putting in place the procedures we need to prevent fraud and to ensure Ireland retains its reputation as a first-world economy and as a probusiness environment. At the company level, we’re complying with the enhanced reporting and regulatory requirements. And I think it’s fair to say that compliance and regulatory matters are demanding more and more time from the senior officers and from audit committees throughout the country.

Originally published July 2006.

Duties and Responsibilities

Prevent, Detect, Respond: Taking Corruption Seriously

By David Van Homrigh, National Managing Partner, Forensic, KPMG in Australia

It's sometimes said that what we don't know can't hurt us. That's a dangerous illusion when it comes to corruption.

In many countries, bribery to conduct business poses major legal and reputation risks to companies at home and abroad. Countries like Australia, which was ranked the world's ninth-least corrupt country in Transparency International's "2006 Corruption Perceptions Index," are not immune to corruption and fraud.

Corruption is a serious, but often unrecognized risk for many organizations. For instance, The World Bank has estimated that more than U.S. \$1 trillion in bribes are paid worldwide each year.

A recent study by the Centre for Australian Ethical Research found that only half the companies in the S&P/ASX Top 100 have policies explicitly banning the giving and receiving of bribes, compared with 92 percent in the UK and 80 percent in the United States.

Corruption and bribery need to be confronted at a board and senior management level. A company should develop and promulgate clear, firm policies on what constitutes corrupt conduct and steps to prevent it. KPMG in Australia recommends adoption of a "prevent, detect and respond" approach to corruption.

Prevention of corruption is as much about organizational culture as it is about rules and control systems. Compliance is more than paper shuffling. It is about creating an ethical culture in which corrupt behavior stands out as a detectable aberration.

Australian organizations are sometimes exposed to corrupt activities when they venture offshore. KPMG's "Fraud Survey 2006" revealed that Australian and New Zealand companies with operations in Asia were far more likely to suffer problems with kickbacks and bribery than their counterparts back home.

Companies doing business offshore – especially in Asia, Africa, the Middle East, Eastern Europe and South America, according to Transparency International's 2006 Bribe Payer's Index – need to recognize that corruption is likely to be an issue they can't ignore. They need to resist the temptation to regard bribes, kickbacks and other illicit payments as a "cost of doing business" in some places.

Some suggest that by facilitating commercial activity, corruption actually encourages growth. Perhaps, although there's mounting evidence that corruption retards growth, entrenches poverty and inequality and undermines investor confidence. It is almost certainly no mere coincidence that many of the world's poorest, least democratic and worst-governed states are also the most corrupt.



In any event, Australian companies have more than just moral or ethical reasons for taking corruption seriously.

It's difficult to argue that globally, corruption is being rolled back. Indeed, the reverse may be the case.

Nevertheless, there's a concerted, worldwide reaction against corruption evidenced in the many international conventions and treaties calling on governments to take effective action to deter, detect and respond to corruption. Many countries are introducing their own complementary laws covering corrupt payments made by their nationals in other countries.

In Australia, the Criminal Code Amendment (Bribery of Foreign Public Officials) Act 1999 makes it a criminal offense to bribe a foreign public official, whether it occurs inside or outside of Australia. The Act is the result of Australia's ratification of the Organization for Economic Cooperation and Development's (OECD) Convention on Combating Bribery of Foreign Public Officials in International Business Transactions 1997. Organizations and individuals can be charged under Australian law on foreign bribery if they have:

- Intentionally, knowingly or recklessly committed the offense
- Expressly, tacitly or impliedly authorized or permitted the commission of the offense
- Worked in a corporate culture that directed, encouraged, tolerated or led to noncompliance with the law, or
- Failed to create and maintain a corporate culture that required compliance with the law.

Under Australia's foreign bribery law, individuals can be criminally responsible for failing to create and maintain a culture that requires compliance; it significantly extends the scope of corporate criminal responsibility beyond the position at common law.

Likewise, an offense can be committed without a bribe actually being paid: offering or promising a corrupt benefit (including non-monetary and intangible inducements) in contravention of the law is sufficient. This law also covers bribes paid or offered via intermediaries.

The Income Tax Assessment Act 1997 also prohibits tax deductions for bribes to foreign public officials, but allows deductions for "facilitation payments" made for "expediting or securing the performance of a routine government action of a minor nature." These minor facilitation payments are also permitted under the Criminal Code, although it's unclear exactly when a facilitation payment turns into a bribe.

Although there are doubts over the real-world applicability of Australia's foreign bribery laws, sooner or later they're likely to be tested in some high-profile cases. Australian organizations could also face criminal and civil liabilities under foreign anticorruption legislation, including the U.S. Foreign Corrupt Practice Act of 1977.

Remember, too, that corruption cases threaten companies with far more than financial loss. The Cole Inquiry provided dramatic proof of the way allegations of corruption can destroy corporate and individual reputations.

Serious corruption charges undermine corporate credibility across the board.

Consider the possibility of criminal charges against directors, senior executives and other employees. Depending on the jurisdiction, entities found guilty of corruption can lose contracts, forfeit assets and licenses, and find themselves excluded from government assistance and purchasing programs.

In addition to prevention and detection, a firm, consistent response to detected corrupt behavior is imperative – irrespective of the materiality of any prohibited payment.

Under Australia's foreign bribery law, individuals can be criminally responsible for failing to create and maintain a culture that requires compliance.

Red Flags That May Signal Corruption

Organizations that answer any of the following questions in the affirmative could be vulnerable to corruption:

- Does the organization operate in industries or countries with a reputation for corruption?
- Have offshore agents, consultants or other intermediaries been engaged to obtain regulatory approvals, permits, licenses, etc.?
- Is the organization discovering undocumented payments, "mis-labeled" transactions or poorly substantiated disbursements of consulting fees?
- Are individuals discouraged from reporting concerns about corruption, or simply not informed about how they should go about doing so?
- Is policy on corruption regarded as sensitive information that's communicated only to a select group of high-level executives?
- Are foreign business partners screened for their financial status, but not for their commercial probity?
- Is the organization making payments directly to foreign government officials? Are intermediaries being paid to "facilitate" the cooperation of officials?
- Are payments being made on behalf of foreign officials for expenditures that appear private in nature, including such items as travel expenses, school fees or golf club memberships?

Originally published May 9, 2007.



Duties and Responsibilities

Corporate Governance Convergence Is a Global Problem

By Andrew Rosenbaum, Contributing Editor, *Audit Committee Insights International*

The difficulty in converging international accounting standards points to a larger issue for audit committees: nascent efforts to converge corporate governance leading practices from around the globe.

Some observers support the development of uniform corporate governance principles that apply to the culture of an organization rather than standards that prescribe the structure of companies, says Tim Copnell, director of KPMG's UK Audit Committee Institute (ACI).

"It's difficult to see a wholly unified approach in the short- to medium-term, given the cultural and historical differences in the governance world," Copnell says. "One only has to look at the problems encountered in efforts to harmonize accounting standards, between international accounting standards, national standards and U.S. standards."

Global standardization of corporate governance practice has lots of hurdles. "Such a move would not take into account fundamental cultural and legal system differences; one could not impose the creation of a given culture on the entire world in this sensitive area," agrees Patricia Peter, corporate governance expert at the Institute of Directors in London.

"The British system, with its essential 'comply-or-explain' principle, would not tolerate prescriptive legislation like Sarbanes-Oxley. Nor would the British system work well in Germany, for example," Peter says.

In the United Kingdom, "comply or explain" means companies that don't comply with the British Combined Code have the right to explain why they choose not to do so.

"Instead, such a move would be likely to smother innovation, and the adoption of improved practice: today, one culture is free to borrow better practice from another, or to adapt it to fit its own system, but that would not be possible with global prescriptive standards."

Guy Jubb, an investment director and head of corporate governance at Standard Life Investments Ltd. in London, says flexibility has to be built into the process.

"It is important that companies have the flexibility to adjust and tailor their governance to their particular requirements, in a form consistent with entrepreneurial leadership," Jubb says.

Peter believes more than principles need to be taken into account.

"It is so easy for the industry to agree on principles, but the principles take different forms due to the system in which they are applied," Peter says. "Consider that in the U.S., [institutional] investors are treated very differently from retail investors.

This makes it very hard for UK companies to make the same offers to all of their shareholders in the U.S.”

The European Commission has, in fact, restricted its initial plan to impose EU-wide standards of corporate governance.

“The commission had originally intended to impose standards via directive, but now the plan is only to legislate on specific areas like that of shareholders rights,” explains Christopher Pierce, CEO of the London-based Global Governance Services Ltd., which trains audit committee members in corporate governance leading practices and advises regulators around the world in formulating corporate governance codes.

As KPMG’s Copnell points out, “Of the 24 codes in the EU, it does not matter that Germany has two-tier boards, the UK has unitary boards and France has a choice of a unitary or two-tiered board, as long as those boards operate on good principles in a transparent manner, are well informed and have good information.”

The biggest fear is that not only will a global corporate governance regime be too limiting, but will be universally applied to all companies. A common issue is that boards respond to the call for “good governance” by box-ticking rather than managing the business in the best interests of the shareholders and providing them with clear, complete and accurate disclosures as to how this is done, Copnell explains.

Jubb says that flexibility with accountability is the ideal. “[It] works provided that there is proper and appropriate accountability to boards, and that everyone plays their part,” he says.

In fact, it is the global markets and global commerce that should drive improvements in corporate governance around the world, Pierce says.

“If people operating in capital markets take the lead, it will require all participants to continue to improve and reach what is considered to be [a leading] practice,” he says.

Pierce points out that it is difficult to achieve a consensus on corporate governance issues even within the UK.

“There are more than 150 professional organizations here involved with the topic, and considerable differences of opinion between them,” he says. “Consider how difficult it would be to achieve any kind of consensus with their homologues in the U.S., or in Europe.”

Copnell adds that self-regulation also needs to be matched with enforcement. “Any code is essentially useless without an enforcement procedure to make

companies apply them responsibly,” Copnell says.

“In Europe there are new amendments that require all European companies to state the extent of their compliance with a code and to name that code. This mechanism is a step in the right direction, but success ultimately depends on behavioral aspects of companies rather than compliance.”

Originally published February 14, 2007.

“It’s difficult to see a wholly unified approach in the short- to medium-term, given the cultural and historical differences in the governance world.”
—Tim Copnell, director of KPMG’s UK Audit Committee Institute



Risk Management

What ERM Means for Corporate India

By Sammy Medora, Chairman, Audit Committee Institute, India

It has long been believed that a successful risk strategy is to optimize risks, not to minimize them. It is true that companies today are more risk-averse than they were before 2001, when a large number of corporate scandals rocked the world and led to the collapse of world-class companies.

These events led to the enactment of the Sarbanes-Oxley (S-O) Act of 2002 in the United States and also contributed to the birth of our very own Clause 49 of the Listing Agreement in India.

Risk is the uncertainty of an event happening and the consequences if it does. Risk lies in every area of a company. While risk need not result in an adverse outcome, it often produces unpleasant surprises. Yet, when you think about it, if few risks are taken not much business would get done.

So every company needs to find the optimal balance between risk and control, that is its risk appetite, and draw the boundaries for the business risks it will take to advance the company. A more imaginative, optimized approach to compliance with Clause 49 can unlock the potential business value of the regulations and seek to realize that value while still satisfying the regulator.

Corporate governance is often defined as a system that directs and controls corporations. It encompasses three main things: compliance, audit and risk management. In India, enterprise risk management (ERM) has been voluntarily embraced mainly by multinational companies and financial institutions.

Other listed companies are now forced to embrace it to comply with Clause 49; this has brought about renewed focus on ERM and CEO/CFO certification of internal control effectiveness. Indian listed companies have begun to realize that ERM is not a passing fad, but is here to stay as an integral part of the corporate governance process.

Some feel uneasy that many Indian companies may throw money at creating a bare minimum compliance solution that follows the letter of the law but not its spirit. The point they might easily miss is that companies can extract increased operational efficiencies when they undertake compliance constructively, for many of Clause 49's compliance requirements are simply "best practices" turned into regulations.

No doubt those regulations will drive compliance in the vast majority of companies listed in India.

But isn't it odd that a high-impact regulation on risk management is buried in Part IV of Clause 49 under the heading "Disclosures" and is only 36 words long? It reads, "The company shall lay down procedures to inform board members about risk assessment

and minimization procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework.”

Several audit committee members of Indian companies have mentioned that they would like the Securities and Exchange Board of India (SEBI) to specify some ERM framework and guiding principles and standards for companies to follow in developing their ERM plans.

Other audit committee members feel Corporate India is sufficiently knowledgeable about ERM. They feel it already is an integral part of their companies and SEBI should only provide the broad regulatory framework for companies to function in this area. Whatever their preference, because Clause 49 provides a short, high-level requirement for risk management, companies will need to turn to best practices to fill in the lack of detailed requirements.

So what is ERM?

ERM entails assessing and monitoring risks from numerous sources; the ultimate goal of ERM programs is to increase shareholder return.

In India since 2001, ERM has evolved steadily in progressive companies. It is developing from being merely a risk identification and assessment process to building a risk portfolio that is continually assessed and monitored.

The perception that “risk is not my responsibility” has evolved to a more realistic view that “risk is everybody’s responsibility.” These changes have resulted in ERM becoming an integral part of a company’s operating philosophy.

A company’s success in managing risks comes from its corporate culture. Audit committee members should be alert to changing trends within an industry and should have adequate policies and procedures to embed good corporate culture.

Directors and senior management must understand their company’s fundamental business and inherent risks. They should understand and communicate the tradeoffs between risk and reward, and have a strong sense of how much is too much. As this message is delivered it should help everyone in the company understand how to balance short-term gains with long-term goals.

The board and management could simulate different situations and problems that may be faced by the company and suggest how to deal with them. This would enhance awareness and improve the quality of management.

Some feel uneasy that many Indian companies may throw money at creating a bare minimum compliance solution that follows the letter of the law but not its spirit.

Audit committee members should be alert to changing trends within an industry and should have adequate policies and procedures to embed good corporate culture.

The board should set the tone for integrity within the company and ensure that it permeates to grass root levels. The audit committee should also ensure that the policies laid down by it are complied with, since shareholders could hold the board accountable as an oversight body that looks after their interests.

Choosing the right management to run the company is an important step to minimize the risk of fraud. Another important element of governance is to ensure the company has an adequately robust system for escalating matters by employees to appropriate levels (a whistle-blower process).

The board and its audit committee should put in place ethics and compliance policies and also suggest procedures for how the company should go about managing and monitoring the risks of fraud within the company. Helping to ensure that the right people are hired for the right job is a good way to help minimize the risk of fraud.

ERM is primarily management's responsibility. The board and senior management have long sought ways to better control the companies they run.

Internal controls are often put in place to keep companies focused on profitability goals and achievement of their mission, and to help minimize unpleasant surprises along the way. Since Clause 49 also requires management to implement procedures to inform the board about the risk assessment and minimization processes, these processes should be periodically reviewed to help ensure that management controls risk through an in-depth, defined, designed and implemented framework.

The board of directors, being the highest body in the corporate governance hierarchy, is primarily responsible for defining the risk management framework and for ensuring that risk management applies to every level within the company.

While the implementation of policies and procedures should be entrusted to management, the board should always consult with management to determine the key risks that could impact the company and its operations. Because the reputation risk of a company lies with the board, the primary accountability of risk management oversight also lies with the board.

There will be a fine balance between risk and control for a company to function well. The board and its audit committee should understand the key elements of ERM, question management about risks, and concur on major risk management decisions. However, they should neither make choices on behalf of management nor assume management's role in ERM.

The level of risk that a company is willing to accept is management's decision and generally there can be no right or wrong decision.

There are several ERM frameworks to choose from, of which the integrated ERM framework of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) appears to be the gold standard for implementing risk management.

It describes a direct relationship between objectives (what an entity strives to achieve) and ERM components (what is needed to achieve them). This relationship is portrayed as a three-dimensional cube, with eight interrelated components that fit in well with Clause 49's requirements.

COSO's flexible framework allows a company to focus on the entirety of its ERM framework, or by objectives category, components, entity unit, or any combination thereof.

ERM can be used by management as an effective decision-making tool. The key things that ERM does are help drive information and better decisions, which in turn drive better financial results and improved shareholder value.

ERM requires a company to systematically identify and assess the risks throughout its operations, factoring in both external and internal factors. Risk management processes inform senior management about the company's risk profile and likelihood of achieving its long-term goals. ERM helps in effective reporting and compliance with laws and regulations and it also helps avoid damage to the company's reputation and associated business consequences.

ERM is the means, rather than an end, of good corporate governance. With the right perspective and knowledge, sensible Indian boards will be able to leverage the significant effort and technology investments made in the name of compliance with Clause 49 to further their mission to deliver increased shareholder value.

The board and its audit committee should understand the key elements of ERM, question management about risks, and concur on major risk management decisions.

Originally published September 13, 2006.



Risk Management

Audit Committees: Decide on Who Does What in Risk Management

By Andrew Rosenbaum, Contributing Editor, *Audit Committee Insights International*

Like many of their brethren around the world, audit committees in Canada find themselves in the middle of a critical debate over who has responsibility for risk management oversight.

While the audit committee's responsibility often is not clear cut given the range and complexity of risks facing companies today, Canada has its own regulations regarding this matter.

In Canada, unlike the U.S., regulations do not specifically require audit committees to be responsible for discussing guidelines or policies to govern the process for risk assessment or risk management.

Yet many audit committees in Canada are recognizing the need for a defined process that enables them to effectively oversee financial reporting risks and other compliance matters. For other risks that audit committee may or may not have oversight responsibilities, they are increasingly playing the role of "catalyst" to help ensure key risks are being overseen by someone.

According to a KPMG Audit Committee Institute (ACI) 2006-07 global survey of public company audit committee members, more than 60 percent of the respondents indicated that risk management oversight will be one of the highest priorities on their audit committee agenda for 2007.

"Audit committees need to understand 'who does what' in risk management oversight," says Michael Meagher, the executive director of KPMG's ACI in Canada and a partner with KPMG in Canada's Toronto office. "Otherwise, the subject lends itself to endless debate – and critical risks can fall through the cracks."

Audit committees, says Meagher, have to be careful not to cross the line between risk management oversight and direct risk management.

"To do this properly, a formal risk management oversight process should be articulated," says Brian Gibson, head of the Accounting/Audit Subcommittee for the Toronto-based Canadian Coalition for Good Governance. "In this way, the limits of the audit committee's responsibilities will be clearly defined."

Ian Giffen, a board member at technology companies Corel Corp., MKS Inc., and Descartes Systems, says risk management is a relatively new business practice.

“Generally risk management is still an emerging practice, often lacking a common vocabulary, consistent context, and formal framework,” says Giffen, a former audit committee member at other public companies including Macromedia. “A well-defined checklist approach, combined with a robust dialogue, can keep risk management in focus.”

Likewise, says Meagher, the audit committee needs to have a clear understanding of its oversight responsibilities, and a structured approach for overseeing the company’s risk management efforts – particularly in those areas affecting the financial reporting process.

“The first step is for the audit committee to review its charter to ensure the committee understands the scope of its risk oversight responsibilities – and that its oversight activities correspond to those responsibilities.”

Over time, the diversity of opinion about the audit committee’s role in risk oversight may narrow with the evolution of oversight practices, regulatory guidance, and perhaps court decisions on the matter, Meagher says.

“For now, leading audit committees are taking a common sense – and prudent – approach to determining which risks are, or should be, within the committee’s purview,” Meagher says. And for those risks that are not their responsibility, audit committees figure out who is responsible and how potential financial reporting risks owned by others are communicated to the audit committee.

In Canada, primary oversight responsibility for the company’s financial reporting and disclosure process rests with the audit committee. “A company’s risk management efforts are critical to the audit committee’s oversight of the financial reporting process because some non-financial risks have financial reporting implications,” Gibson says.

Meagher believes strong risk management can help the audit committee ensure that for each significant risk there is a good control and disclosure process. That calls for making sure there are appropriate internal controls, that management makes appropriate disclosures regarding such items as presenting critical accounting estimates and judgments in management’s discussion and analysis, and that the financial statement impact of the risk is properly recorded.

Audit committees also oversee other tasks that should consider risk, including the certifications that the CEO and CFO are required to make on the company’s financial statements and internal control, as well as the internal and external audit plans, Meagher says.

“Audit committees need to understand ‘who does what’ in risk management oversight.”

—Michael Meagher, executive director of KPMG’s Audit Committee Institute in Canada and partner with KPMG in Canada’s Toronto office

“A company’s risk management efforts are critical to the audit committee’s oversight of the financial reporting process.”
—Brian Gibson, head of the Accounting/Audit Subcommittee for Canadian Coalition for Good Governance

Giffen explains that, in its oversight role, the audit committee should have a good understanding of, and level of comfort with, the company’s process for identifying, managing, and reporting risk. This process should help the audit committee obtain a clear picture of the company’s risks, and its risk management approach.

He says the information generated by this process should include identifying and prioritizing significant risks, quantifying the financial implications of each risk, determining who has primary responsibility for management of specific risks and evaluating the status of management’s risk mitigation efforts.

Certain risks that are more “qualitative” in nature, such as management inexperience or misalignment of employee incentives and strategy, can be difficult to quantify or translate into financial terms, Meagher says. Nevertheless, management should have a method for reporting these types of risks to the audit committee.

The board or the audit committee must demand relevant, timely and accurate information from senior management, the internal auditor, and the external auditor, to ensure it is meeting its oversight responsibilities, Gibson says.

In addition, the board or the audit committee needs to assess periodically whether they are receiving appropriate risk management information, regularly enough, and in a format that meets their needs, Meagher says.

He also believes they need to evaluate, at least annually, the adequacy and timeliness of management reporting to the board or the committee on financial, nonfinancial, current and emerging risk trends.

“Clearly, audit committees are devoting more time to ensuring that they understand the company’s risk management process and what their oversight responsibilities are,” Meagher says. “And it’s time well spent.”

Andrew Rosenbaum is a London-based journalist who writes frequently on business and finance.

Originally published May 9, 2007.

Financial Reporting and Internal Controls

Sustaining Financial Controls That Contribute to Business

Editor's Note: This commentary represents the views of Jakob Baer, an audit committee chairman for Swiss Re, and Paul Meeusen, a managing director for internal audit at Swiss Re. Baer is the former CEO of KPMG in Switzerland.

To keep financial reporting under control, companies need to view internal controls over financial reporting as they work on their core business, and audit committees need to oversee this process.

An internal control system can only add value if management gets involved, understands and takes ownership of business processes and controls. Without such an approach, the controller's work becomes unpleasant – and audits and control verifications become painful.

This article summarizes some of our experiences with internal controls in reinsurance.

Shareholders of some Swiss insurance and reinsurance companies have had to contend with unfavorable returns. Despite corporate efforts to restore balance-sheet quality, investors and analysts remain fairly skeptical about the industry, in part due to the perceived lack of reinsurers' earnings transparency.

Accounting anomalies haven't simplified matters, nor have accounting regulations. Meanwhile, more reinsurance transactions involve sophisticated structures, combining elements of risk finance, risk transfer, cross-border variable interest entities, layers of retrocession arrangements and securitization. All this in turn requires advanced accounting treatment and robust financial reporting operations.

In addition to accounting issues, reinsurers must consider the fight for talented individuals. The growing workload of compliance and financial control has increased demand for highly qualified financial and accounting professionals, in an environment where costs are already under pressure.

All this poses challenges to a reinsurance chief financial officer, who has to maintain adequate controls while reigning in costs and attracting and retaining top-flight professionals.

Any strategy aimed at establishing a strong financial control framework needs to start with a company's duty to deliver reliable financial information to shareholders. We suggest a strong financial control strategy has to start with transparency of business and financial reporting processes.

Business professionals – underwriters, client managers, claims and investment specialists – need to share and review business processes, and identify the key risks and controls for financial reporting. And finance professionals have to provide oversight and infrastructure needed in an efficient and low-maintenance manner.



Any strategy aimed at establishing a strong financial control framework needs to start with a company's duty to deliver reliable financial information to shareholders.

Any internal controls project should start by management identifying the key business processes in the value chain.

How can reinsurers turn strategy into action? It starts with aligning interests.

Managers tend to be interested in financial figures that drive their performance evaluation. Reinsurance managers often focus simply on the underwriting result or “economic profit.” It is challenge for reinsurers to have fully aligned interest in published financials across the enterprise.

This does not imply that all reinsurers have to become accountants; but it does imply that they need a basic understanding of how everyone in the firm influences accounting figures.

In addition, how can reinsurers and accountants view their financial-reporting work as a common duty? Most managers are still driven more by organizational charts than by business processes, and process owners and their performance metrics are often not visible in the corporate hierarchy.

However, controls can become counterproductive if they slow down a process. Controls should facilitate orderly collection of premiums, payment of client claims and well the reliable production of financial statements for the investor.

Any internal controls project should therefore start by management identifying the key business processes in the value chain and how they contribute to the financial reporting process.

When an internal auditor is required to give an opinion on internal controls as per the recently amended Swiss Code of Obligations, that opinion relies heavily on management documentation of end-to-end processes – from the front office accepting a risk all the way through financial statements reporting.

Clear handovers are the joints that hold the process chain together; they need to be transparent. Control documentation should be succinct enough to allow an independent, qualified person to understand it.

In addition, managers may complain – often, rightly so – about the excessive effort involved in documenting and testing controls. Right at the start, management needs to conduct a sound risk assessment, in order to provide some direction for documentation and assurance teams.

It is a common perception that effective control invariably involves lots of detail, but this is invalid.

A proper focus starts with determining material accounts and entities that form the lion’s share of a company’s financial statements. The best way to start this task is by analyzing the structure of the income statement and balance sheet, in order to understand the relative materiality of each section of the accounts.

An industrial company obviously has more fixed assets on its balance sheet, while a financial institution has a preponderance of financial assets. The accounting complexities and controls will differ – the key control areas for the industrial company will include inventory controls, the valuation of intangible assets and depreciation, while the financial institution's key control areas include the fair valuation of reserves and financial assets.

However, a risk assessment of financial misstatements needs to balance quantitative measures of materiality and coverage. Risk factors include the complexity of calculations or accounting rules, the degree of estimates involved, the potential for fraud and the dependency on complex IT applications.

Managers must get involved in the risk assessment. If risk assessment is carried out in a rigorous manner, it will focus on areas that really matter. It is good practice to track the number of controls identified by key segments of the business, and to verify whether it is commensurate with the materiality of these segments.

How can you ensure that the control system works? For an internal controls certification, which verifies the effectiveness of a company's controls, testing controls is a standard audit verification procedure. But our experience shows that the challenge lies in deciding how strictly to interpret the results.

For example, imagine an X-ray machine at the airport that often fails to detect metal objects. To compensate, screeners would manually inspect the baggage of one in three travelers.

Would this be accepted as a safe set of controls? Certainly not in today's environment. This illustrates that compensating controls (the manual inspection) cannot dispel the fact that the primary control (the X-ray machine) has failed.

In financial reporting processes, primary controls are often of a transactional nature and include verification of contractual documents or reconciliation procedures. Periodic management reviews may compensate for such controls; however, when certain controls fail, management needs to consider the context and determine whether the overall control environment is adequate.

Sound controls and strong governance need to operate in a cost-effective and sustainable manner. Controls cost money and often lose discipline once installed.

Keeping controls in order is management's responsibility. Although control and operational risk teams – and internal and external auditors – provide support and conduct independent tests, it is management who is ultimately accountable for the adequacy and effectiveness of controls.

In financial reporting processes, primary controls are often of a transactional nature and include verification of contractual documents or reconciliation procedures.

Most firms have an internal control system. However, obtaining one that can be understood and audited by a third party is a large undertaking.

We have four final recommendations for a sustainable control environment:

Promote creative process thinking: Establishing internal controls is not process reengineering, but can help devise simpler, standardized new procedures. In the reinsurance industry for example, how could information flow be simplified between cedents and reinsurers who process, re-enter, verify and reconcile the same financial and administrative data?

Offer incentives: Better control can also mean more business. Large reinsurance and capital market transactions often bring additional reporting requirements. Having such processes and controls documented and in good order enables more fluid transaction closing. It also avoids administrative or regulatory surprises after a deal closes.

Origination teams should have incentives to consider reporting and control implications when closing large and complex transactions, particularly with regard to securitization transactions, where this reporting obligation also may extend to the capital markets.

Manage the relationship with your auditor: This has nothing to do with influencing the auditor's independence. Rather, we suggest an open exchange of thoughts with the auditor throughout the definition and maintenance of the control environment.

This allows the auditor to validate the scope and approach early, and to prepare the best-qualified audit team. Open dialogue may also extend to regulators.

Rotate staff: The ideal person to introduce sound internal financial reporting controls has an audit and risk management background, solid finance and accounting skills, a deep understanding of the business and an aptitude for processes analysis and reengineering. Unfortunately, that mix rarely exists in one person.

But this problem can be overcome by actively rotating staff between business, finance and audit or operational risk management teams. This helps increase the acceptance of a control system across the firm, while gaining commitment to the task.

Most firms have an internal control system. However, obtaining one that can be understood and audited by a third party is a large undertaking. To ensure that such a system focuses on the essentials, executive management needs to actively supervise the management of such an initiative. This can lead to simplifying processes through thinking about the controls that are really key.

This is an ongoing and dynamic process, since a control environment needs to be maintained and adjusted to the firm's development. Work does not stop with the initial certification of controls.

Originally published June 6, 2007.

Financial Reporting and Internal Controls

Making the Control Environment Relevant in a New Regulatory World

By Mauro Palazzesi, Partner, Internal Audit Services, KPMG in Switzerland

Internal controls have suddenly moved to the center of attention not only because of the standards of the Sarbanes-Oxley Act but also the ensuing European regulatory framework – from a Swiss point of view, particularly the revised Code of Obligations. These internal controls thus need to be clearly defined and structured.

The COSO (Committee of Sponsoring Organizations of the Treadway Commission in the U.S.) model is becoming increasingly accepted. The control environment plays an important role.

It raises various questions: What is the control environment all about? What are the relevant prerequisites? What are the benefits of a clearly and properly defined control environment?

Constituents of the control environment

The control environment comprises:

- Integrity and ethics
- Commitment to technical requirements
- Role of the top management
- Management philosophy and appearance
- Organization
- Assigned competencies and responsibilities
- Human resources strategies and policies

Integrity and ethics

First and foremost is the management's role model function. Sophisticated controls are useless if they are ignored or not observed by management.

Management at all levels must emphasize the meaning of integrity and ethics, primarily through adequate business conduct. This includes different levels of interaction with staff members, clients, suppliers, competitors and the public.

The most important principles regulating internal and external business conduct should be clearly stipulated in a code of conduct.

Besides defining the corporate values, it is also important to define the necessary consequences of violating the values. Any sanctions need to be communicated. This always offers an excellent opportunity to refer to the desired situation and appropriate conduct. At the same time, it helps to demonstrate that certain digressions from the rules will not be tolerated.



The most important principles regulating internal and external business conduct should be clearly stipulated in a code of conduct.

In this context, the significance of targets and incentives needs to be taken into consideration. Unrealistic targets and poorly thought out incentives may tempt staff members to commit objectionable acts. This could happen if targets cannot be achieved or only be by illegitimate means or if the incentive seems to warrant exposing the business to excessive risks.

After all, it is management's responsibility to make sure that possible violations of standards are properly reported and addressed. Whistle blowing in this context gives rise to numerous discussions: irrespective of its pros and cons, there has to be a tool providing an adequate process of reporting and addressing misconduct.

Commitment to professional requirements

Management defines the professional requirements. They must be aligned to the business purpose and activities. This helps prevent misconduct related to a lack of professional knowledge and experience. Therefore, senior management has to specify the following:

- Business purpose and activities
- Form of organization
- Professional/technical skills requirements
- Management and staff

Practice shows that where the required level of professional skills and organizational structures are defined by the prevailing skills level of the current staff and of management, rather than being based on a sustainable business strategy, the internal control is weakened.

The role of senior management

The board of directors is responsible for the internal control system, even if certain tasks are delegated to the operative management.

What are the prerequisites for the board of directors to be able to assume the relevant responsibilities? The following components are vital for managing effectively:

- Segregation of powers
- Technical skills and time requirements
- Direct communication
- Reporting
- Definition of salaries and the budget for audit activities
- Monitoring the implementation of agreed upon measures

- Segregation of powers within corporate governance is a prerequisite for effective internal control. In order to establish the necessary distance to the executive management and to perform the intended supervisory function, the board of directors must not be involved in the operational management.

The requirements, both in terms of skills and time, are increasing for board members. As a result, for many organizations, it is becoming more important that boards of directors create support committees, like the audit committee, to help them manage their workload.

Particularly the involvement of an audit committee is now considered a leading practice. Nowadays, it is expected that an audit committee has sufficient financial and accounting knowledge, to be familiar with internal and external audit, and to be internal control-literate. Those are some of the criteria for assessing the audit committee's effectiveness.

Another integral part of an active control environment is the effective communication between the board of directors and the audit committee on the one hand, and the internal and external auditors and the CFO on the other hand. A potential executive management filter can thus be eliminated and open and unencumbered communication assured.

Reporting to the board of directors represents a special topic. In practice, line management and internal audit can define the content and frequency of reporting. However, the board of directors should seize its oversight responsibility and define what it receives and how frequently.

Management philosophy and appearance

The philosophy behind management operations represents an essential aspect in efficient controls. Management through its conduct provides certain principles as well as expectations regarding the treatment of internal controls for staff members.

Furthermore, management has to define the structures that provide assurance as to compliance with the specified principles. A code of conduct provides a basis for this.

Organization

The organizational structure has to support the internal control system. This is done through management's clear assignment of tasks, competencies, responsibilities and reporting. In addition, the organization has to be defined pursuant to the requirements of effective internal control systems and to adapt to changing conditions on an ongoing basis.

The board of directors is responsible for the internal control system, even if certain tasks are delegated to the operative management.

Another integral part of an active control environment is the effective communication between the board of directors and the audit committee.

Assigned competencies and responsibilities

The assigned tasks and their respective competencies and responsibilities have to be in agreement with the corporate goals and management philosophy. The activities of management and staff members are based on corporate goals and are essential for properly running processes and a well-functioning system of business control.

Management is responsible for providing the necessary skills and experience. This enables the assignment of tasks, competencies and responsibilities pursuant to overall corporate goals and strategies to the relevant individuals in their respective functions.

Control environment and corporate culture

Integrity, ethics, professional competence, organizational structure and development, management philosophy and style, corporate and human resources policy, delegation of tasks altogether are important aspects of an internal control system.

Their interrelations also shape and influence corporate culture. A clearly defined, positively designed and properly communicated corporate culture creates a strong management tool and allows for a competitive and performance-enhancing atmosphere.

The corporate culture also leads to a unique type of organization and helps attracting and retaining talents.

A well-designed culture

- Strengthens the identification of staff members with the business.
- Makes debates on principles redundant.
- Supports the identification with corporate targets and strategies.
- Supports internal organizational cohesion.
- Increases efficiency and performance of the business.

Internal control systems and corporate culture mutually require and influence each other significantly. The corporate culture aspect always needs to be taken into consideration when designing and implementing an internal control system. Conversely, when defining the corporate culture it is important to take its impact on the corporate control environment into consideration as it ultimately determines the quality of the internal control system.

Future prospects

The control environment is a multilayered and complex component of the internal control systems. It forms the frame within which the controls are defined and integrated into a single system. So-called “soft factors” are making this task more complicated.

The design of a practical and effective control framework is a crucial requirement for an equally practical and effective internal control system. In discussions about internal control systems this should be one of the major focal points.

Originally published December 6, 2006.

**Internal control systems
and corporate culture
mutually require and
influence each other
significantly.**



Financial Reporting and Internal Controls

French Audit Committees Smooth the Transition to IFRS

By Andrew Rosenbaum, Contributing Editor, *Audit Committee Insights International*

French audit committees are adjusting to new oversight roles, as nearly 7,000 companies across the Continent have been making the transition to the European Commission's new International Financial Reporting Standards (IFRS).

"It's a change of planetary dimensions," says Christian Aubin, secretary of the audit committee at the Paris-based bank BNP Paribas, and member of France's National Council for Accounting. "Audit committees have to learn the mechanics of having the new and the old system in operation at the same time. Nonetheless, in France, most of the companies involved have gotten through it with considerable skill."

Audit committees need to make a robust effort in achieving the transition, Aubin says.

"We programmed many sessions between 2004 and 2005 dedicated to the move," he says. "We identified the key elements and we evaluated the diverse points of impact at the board and management levels."

"Each quarter, IFRS was the central point of the central accounts committee meetings, and we created a supplementary audit committee for each phase of the transition. Changing the information system proved to be the most difficult part of it all."

BNP Paribas also appointed an executive manager to administer the entire transition.

"All this work brought the necessary points for implementation to the attention of management," Aubin says.

The IFRS are a set of accounting standards issued by the International Accounting Standards Board. Many of the IFRS are also known as the international accounting standards (IAS). The purpose of those standards is to create an accounting system that can provide comparable results when used anywhere in the world.

Aubin says the education effort has been key to accomplishing the changeover. Still, there have been conceptual difficulties for the audit committee.

"The new system involves complications that had to be addressed by the audit committee in a number of sessions, with a considerable amount of time spent on debate," Aubin says.

One of those complications was that IFRS is principles-based while many European countries used rules-based accounting.

"The IAS is supposed to be based on simple principles, which are easy to apply," Aubin says. "In fact, it is difficult to elaborate regulations that are based on principles instead of on rules. We understood that the objective of this transition is to be able to make comparisons between companies in different countries."

When it adopted IFRS, the EU touted the advantages of creating a Europe-wide system based on common principles, in cost reduction as well as the general benefits of a unified system.

However, "there are specific problems that arise in adopting IFRS that audit committees should be aware of," says Bruno Flichy, president of the audit committee at the Paris-based construction and concession management firm Eiffage.

"There is a link missing between the grand principles and their application; that is, the body of interpretation [that] is either entirely lacking, or only exists in a rigid form, one that is too rigid for us to use in practice," Aubin says.

"The result was that the audit committee had to communicate regularly with the accounting committee to work out how to proceed, to choose between differing interpretations." (An accounting committee is part of the board in European companies.)

Aubin says international comparisons between companies will prove impossible until there is a uniform body of interpretation in each country. There is a danger that the distance will grow too great between developing a new accounting language, the reality of business administration and public communication. Fortunately, the last phase of the process – the balance sheet and financial results – has not changed, he says.

Flichy says that the concept of fair value, which is important under IFRS, has made life more complex for the audit committee. "The fair value concept has been the most difficult aspect of IFRS for us to adopt," Flichy says.

"[Fair value] has introduced a much larger amount of variability into the accounting process – although it undoubtedly affects financial services providers more than companies like ours. Still, the variations change the size of our available cash and can affect our results."

Didier de Menonville, a partner and head of KPMG's Audit Committee Institute in France, also sees fair value as a volatile issue for audit committees.

"The fair value concept is indeed a complex and difficult one because it has a direct effect on the model for evaluation," de Menonville says. "It creates a rocky road for bankers above all."

Flichy says that the new system has not yet been applied to all areas of business. "Stock options, employee savings plans, and a number of other rather essential areas [are unclear under IFRS]," Flichy says. "We've swum to the middle of the river, but we haven't crossed to the other side."

But IFRS isn't necessarily the cause of change, French audit committee members say, but rather a symptom of all-around alterations in the European business landscape.

"It's not IFRS, it's the overall regulatory environment that has changed over the past five years," Flichy says. "It is this overall process of change, and not IFRS in itself, that has made life more complex for audit committees."

"The new system involves complications that had to be addressed by the audit committee in a number of sessions, with a considerable amount of time spent on debate."

—Christian Aubin, secretary of BNP Paribas audit committee

Originally published June 6, 2007.



Information Technology

For Brazil's Audit Committees, IT Governance Is Here to Stay

In addition to corporate governance, audit committees in Brazil are responsible for the oversight of information technology as it relates to financial reporting. So-called "IT governance" is fast becoming an integral part of audit committees' jobs.

That concept has taken hold in the United States and elsewhere. But in Brazil, which doesn't have a long history of audit committees, how should the audit committee handle IT governance?

Renato Opice Blum and Rubia Maria Ferrao, two lawyers with Sao Paulo-based Opice Blum Advogados Associados, have made a special study of this subject. Blum was a panelist on a KPMG's Audit Committee Institute in Brazil roundtable speaking about this subject.

Blum and Ferrao spoke with *Audit Committee Insights International* about the challenges that audit committees face in Brazil regarding IT governance.

Audit Committee Insights International: How does IT governance enter the audit committee's mandate?

Renato Opice Blum: IT governance is a subset discipline of corporate governance, focused on information technology systems and their performance, and risk management. The rising interest in IT governance is partly due to compliance initiatives like Sarbanes-Oxley and Basel II for banks, as well as the acknowledgement that IT projects can easily get out of control and profoundly affect the performance of an organization.

ACII: Aren't IT matters best handled by specialists in information technology?

Blum: IT can no longer be an area restricted to technicians and professionals. The audit committee, both in Brazil and elsewhere, is responsible for the oversight of financial reporting, and the incorrect management of the IT system could result in non-compliant or inexact financial reporting.

It would be too easy for an audit committee to claim that it was "fooled" by bad information due to non-compliant information technology. The audit committee needs to understand the overall architecture of its company's IT applications portfolio. The audit committee must ensure that management knows what information resources are out there, what condition they are in, and what role those systems play in generating revenue.

ACII: Can you put this into the Brazilian context?

Rubia Maria Ferrao: In the Brazilian legal system, a manager must [make] a diligent effort to control non-compliance. Should management not make such an effort, it is liable not only to fines, but also to prosecution. A company must ensure that it respects the law in order to manage risk properly.

For example, part of risk management is monitoring. If an employee is engaging in illicit activity of some sort over the Internet using the company's information technology system, then the company itself could be held responsible.

So the audit committee should make certain, as part of its mandate to manage risk, that the correct processes for monitoring IT activity have been put into place, and are correctly updated at the company.

ACII: Does this mean audit committee members have to take courses in IT?

Blum: Well, probably not. But the audit committee should be IT-literate, and it should make use of consultants when necessary to [ensure] the company's system is fully compliant, and that the IT system transmits accurate information used in financial reporting.

The audit committee should at least be familiar with the standards involved. BS7799 was created in 1995, by the British Standards Institution (BSI), as a standard to guide the development and implementation of an information security management system, commonly known as an ISMS. [Among other things], it comprises security policy, system access control, operations management, system development, physical security, compliance, personal security and business continuity management.

As the work becomes more technical, they should consult experts.

ACII: Does the situation differ for companies subject to Sarbanes-Oxley, which are listed on American exchanges?

Blum: There is no equivalent to Sarbanes-Oxley in Brazilian law, although several bills under consideration are comparable and may see enactment soon. Companies listed in the U.S. are of course subject to the legislation, and they must use a more severe scheme of compliance. For example, we keep financial records in Brazil for three years, but S-O requires seven years of record maintenance.

“It would be too easy for an audit committee to claim that it was ‘fooled’ by bad information due to noncompliant information technology.”

**—Renato Opice Blum,
attorney with Opice Blum
Advogados Associados**

“The audit committee should make certain, as part of its mandate to manage risk, that the correct processes for monitoring IT activity have been put into place.”
—Rubia Maria Ferrao,
attorney with Blum
Advogados Associados

[For those companies subject to Sarbanes-Oxley], the external auditor should be S-O compliant, and the audit committee must ensure that he is. In terms of IT governance, this means close familiarity with the S-O rules so that compliance is assured.

ACII: Does the rate of change in technology put a particular onus on audit committees?

Ferrao: We all know that information technology is evolving at a terribly rapid rate, and in a very large number of areas. Even trained computing professionals have difficulty keeping up with all of the changes across the industry.

[Several] of the most recent changes involve new forms of communication – instant messaging or Voice over Internet Protocol (VoIP), [for] example. What we have seen is that employees in companies everywhere – not just the technology specialists, but all of them, particularly if they are under 40 – adopt the use of these new technologies very quickly.

Many of them put new technologies to work at their jobs. This makes the potential for non-compliant behavior great, and so the audit committee must be certain that management can keep up with all these changes and innovations. That puts a considerable burden on management, but an even greater one on the audit committee.

Originally published April 11, 2007.

Information Technology

How To Make IT Governance Work for Audit Committees

By Andrew Rosenbaum, Contributing Editor, *Audit Committee Insights International*

By aligning their oversight responsibilities with the rest of the board and being provided with a risk assessment process, audit committees in South Africa and around the world could begin to do a better job with information technology governance, industry observers say.

Just as countries in Europe have the European Union Company Law Directives and the United States the Sarbanes-Oxley Act, South Africa has the King Code, which is that country's corporate governance reform law.

A recent KPMG Audit Committee Institute survey of 1,343 audit committee members in several countries shows that IT governance continues to be one of the most difficult issues for audit committees, but it is still not receiving the attention it requires. More than 90 percent of audit committee members across the globe are "not very satisfied" that their audit committee devotes sufficient agenda time to oversight of IT risk, the survey found.

"Given that capital in our borderless world can be made or destroyed by the click of a mouse, attention to IT governance should be a much greater priority," says Mervyn King, chairman of the audit committee at the Johannesburg-based consumer finance company JD Group Ltd. and chairman of the South African Institute of Directors King Committee on Corporate Governance.

The Audit Committee Forum in South Africa, which is co-sponsored by KPMG, believes that audit committees need to focus on the company's information requirements, and the risks posed by the ways in which the company fulfills those requirements, according to Lindie Engelbrecht, national coordinator of the Audit Committee Forum in South Africa and partner in KPMG's Department of Professional Practice. The demand for more-timely information also imposes risks that need to be managed by the appropriate security measures.

IT governance is defined by a 2005 Information Systems Control Journal as a framework that supports the effective and efficient management of information resources to achieve corporate objectives. It focuses on the measurement and management of IT performance so that related risks and costs are controlled.

In most IT governance structures in South Africa and around the world, the board of directors is responsible for the strategic direction and a decision regarding IT and the audit committee is responsible for the operational aspects of IT, particularly the oversight of IT risks.



**“Given that capital in our borderless world can be made or destroyed by the click of a mouse, attention to IT governance should be a much greater priority.”
—Mervyn King, audit committee chair and head of South Africa’s King Committee on Corporate Governance**

According to the ACI survey, audit committees play an oversight role in three main areas. Those areas are IT risks and controls (66 percent of audit committee members are responsible for IT risks and controls); business continuity (more than 50 percent stated business continuity oversight is a role of the audit committee) and information security and privacy (48 percent stated that information security and privacy was part of their IT governance role).

Yet despite the extensive responsibilities that audit committees take on for IT governance, many audit committee members and other directors do not actually have the working understanding of the technology that would enable them to perform their oversight roles.

In South Africa, corporate governance principles are elaborated in the King Code of 2002. Section 5.3 of this code requires the management board set up a system of controls for information and communication.

That section of the code covers IT and all the channels of communication that it creates. The management board is responsible for monitoring compliance in this area, and for making oversight of the monitoring process available to the audit committee.

Audit committees and boards need to align their oversight responsibilities for IT governance and agree on an arrangement that makes the most sense for culture and governance structure of the company, according to the Audit Committee Forum in South Africa. This should clearly be addressed in the charter of the board and the audit committee.

Robert Lumb, a member of the audit committee at Cape Town-based specialist retail group New Clicks Holding and liquor maker Distell Group (both listed on the Johannesburg Stock Exchange), points out one area where such role division can fail.

“When the IT department installs a new or upgrades an old system, the risks associated with the change are considerable,” Lumb says. “Responsibility for governance around these risks usually rests with the board, the risk committee, and the audit committee.

“What often isn’t defined is which of these three bodies has the ownership of the governance of these risks.”

The division of responsibility here should be clear cut, as is the resources that the audit committee makes use of to complete its oversight role.

“Audit committees should also utilize the resources available within the company to provide the relevant appropriate information and education regarding IT risks and assurance with regards to IT controls,” Engelbrecht says. This information is provided through the CIO as well as internal audit and external audit support.

To achieve effective and efficient risk management, a quantifiable objective and quantifiable assessment of all significant risks is needed.

An audit committee should therefore be provided with a framework for assessing IT risks, Engelbrecht says. One of the most internationally recognized framework is the Control Objectives for Information and related Technology (COBIT), a set of best practices for IT management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992. The COBIT framework is regularly revised to make it a solid point of reference for audit committees, Engelbrecht adds.

Effective communication will assist the audit committee in fulfilling its oversight responsibility. Once management has assessed and mitigated the key IT risks by designing and implementing appropriate controls, management must then create a channel of communication which brings all of these controls to the attention of the audit committee.

The audit committee should then be able to evaluate whether or not the controls are adequate and operative, Engelbrecht says.

Originally published July 4, 2007.

**“Responsibility for governance around these risks usually rests with the board, the risk committee, and the audit committee.”
—Robert Lumb, audit committee member with New Clicks Holding and Distell Group**



Information Technology

As Technology Committees Grow, Audit Committees Lend a Hand

By Gary Larkin, Managing Editor, *Audit Committee Insights International*

As more companies use technology to operate their business and monitor their internal controls over financial reporting, boards and audit committees are realizing they need a clear oversight process for IT governance and risks.

A clear allocation and alignment of information technology (IT) oversight responsibilities is fast becoming everyone's worry as companies try to avoid the "train wreck waiting to happen," also known as bad IT governance, according to Richard L. Nolan, chair of the information technology committee and member of the compensation committee of software provider Novell.

As for IT risks that directly affect financial reporting, there are quite a few. In addition to those risks associated with automated internal controls over financial reporting, there is the consolidation of accounting systems following a merger or acquisition and business continuity and disaster plans that rely on computer and software backup for data centers.

"Audit committees have the responsibility for oversight of IT risks associated with financial reporting, including compliance and internal controls risks," says Kenneth Daly, executive director of KPMG's Audit Committee Institute.

"This oversight responsibility includes asking questions about how investment decisions are made, how IT strategy supports business strategy as well as the role of internal and external resources."

The end game is that boards and management want to avoid the inefficiencies that can cost a company millions of dollars or noncompliance with new corporate governance regulations. Boards should ensure against IT-based surprises, such as project overruns, the "ticking time bomb" computer legacy systems or lax IT internal controls, Nolan says.

An October 2006 *Compliance Week* analysis of 400 companies disclosing material weaknesses in internal control over financial reporting showed that 52 blamed their IT systems on the weakness.

According to the global market intelligence firm IDC of Framingham, Mass., U.S. companies invested \$314 billion in technology in 2005. Another study by AMR Research, a Boston-based advisory firm, found that companies spent \$9 billion on IT compliance costs alone in 2006. That same survey estimates total compliance spending to reach \$28 billion this year.

“What has taken place in the last 20 years is that IT expenses have moved from 1 percent to 10 percent of the budget,” says Nolan, who also is an emeritus business professor at Harvard Business School and a professor of management and organization at the University of Washington Business School.

This focus has brought about the creation of board-level technology committees at some public companies and the expansion of those that have existed already at technology firms, Nolan says. He believes the implementation of the Sarbanes-Oxley Act of 2002 has put more of a focus on the technology committee.

The 2006 National Association of Corporate Directors Public Company Governance Survey reports that the number of companies with technology committees grew to 8.4 percent from 5 percent in 2005.

The growing focus on IT oversight does beg the question of just what constitutes IT governance.

According to the Information Systems Audit and Control Association (ISACA), “IT governance is a framework that supports the effective and efficient management of information resources, which can be people, funding and information.”

ISACA states that the focus is on measuring and managing IT performance to ensure the risks and costs associated are appropriately controlled.

“When you look at IT risk, you should be looking at all business risks,” says Norman Marks, vice president of internal audit for San Jose, Calif.-based software company Business Objects.

“I believe they [the audit committee] should be doing a lot of listening,” says Marks. “Very few audit committees meet with the CIO. They usually talk to the CFO.”

“On a periodic basis, the audit committee should be talking about IT with the CIO, talking about marketing issues with the marketing officer or talking to the general counsel about other risks,” he says.

George Spafford, a principal consultant with Pepperweed Consulting, a Indianapolis-based IT management process improvement firm, believes there is one important question audit committees should ask management.

“I would like to see audit committees asking management why [they are using IT],” Spafford says. “Audit committees have to shift to asking the question, ‘What are the controls?’”

A clear allocation and alignment of information technology (IT) oversight responsibilities is fast becoming everyone’s worry as companies try to avoid the “train wreck waiting to happen.”

“I believe they [the audit committee] should be doing a lot of listening. Very few audit committees meet with the CIO. They usually talk to the CFO.”
—Norman Marks, vice president of internal audit for Business Objects

As a follow-up, audit committees should be more concerned with asking management, internal audit and the CIO if the company is getting what was promised by the technology, he says.

“What’s amazing is how very few organizations require business cases to show they are getting the benefits of what was promised,” Spafford says.

One way audit committees can try to get the answer to that question is by collaborating with the technology committee or in some cases an IT governance committee.

Nolan has first-hand knowledge of how the audit committee and the technology committee work together to provide clear oversight of IT governance and risks.

“There’s a hand in glove relationship,” he says about the relationship. “What you need on the audit committee is someone who understands all the different IT audit processes.”

And a technology committee should have a person versed in IT audit as well, preferably a member of the audit committee, says Nolan.

In two cases where Nolan has been a director, he has seen audit committees that had knowledge of the IT audit process. “One was a CEO for an IT company and another was a CIO for a purchase management company,” he says.

Nolan goes as far as to say that any IT oversight committee’s relationship with the audit committee be very close “because IT issues can affect economic and regulatory matters such as S-O compliance.” He even says the committee’s charter should spell out its relationship to the audit group.

Borrowing a page out of the audit committee’s play book, Nolan says a technology committee should have an IT expert similar to the aforementioned committee’s financial expert.

“The IT expert must have not only a solid grounding in the firm’s overall business needs but also a holistic view of the organization and its systems architecture,” Nolan and Warren McFarlan, a Harvard Business School professor emeritus, wrote in a recent HBS article. “The expert must also thoroughly understand the underlying dynamics governing changes in technology and their potential to alter the business’ economic outlook.”

Originally published February 7, 2007.

If you don't already receive *Insights International*, register today online for your free subscription at www.kpmginsights.com. We also invite you to explore the range of ACI resources—including audit committee forums, surveys, and publications—offered in more than 26 countries at www.kpmgauditcommitteeinstitute.com.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2008 KPMG International. KPMG International is a Swiss cooperative. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved. Printed in the U.S.A.

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.
32186NYO