

## IT governance

### Introduction

The European Audit Committee Leadership Network held its sixth meeting in Paris on 12 May 2006. Members first considered information technology (IT) governance and the associated technology risks and then explored in depth another particular source of risk: major emerging markets.<sup>1</sup>

The French Institut de la Gouvernance des Systèmes d'Information defines IT governance as a: “process based on best practices enabling the business to drive its IT function in order to support its value creation objectives; increase the performance of IT processes and their customer orientation; master the financial aspects of IT; develop IT solutions and competencies needed by the enterprise in the future; and ensure that IT-related risks are managed”.<sup>2</sup>

The network's discussion on IT governance focused on three topics:

- **Five key IT risks**
- **IT oversight by the board and audit committee**
- **Sources of expertise for the board and audit committee**

The members of the network participating in the meeting, or contributing through individual discussions beforehand, sit on the boards of about 50 large, mid and small cap public companies. For further information about the network, see “About this document” on page 9.

Members attending the meeting included:

- Mr Per-Olof Eriksson, Audit Committee Chair, Volvo
- Mr Jan Hommen, Audit Committee Chair, Royal Ahold
- Sir Anthony Greener, Audit Committee Chair, BT
- Mr Daniel Lebègue, Audit Committee Chair, Alcatel
- Dr DeAnne Julius, Audit Committee Chair, Roche Holdings
- Mr Tom McGrath, Global Managing Partner, Ernst & Young
- Mr Christian Mouillon, Global Vice Chair, Assurance and Advisory Business, Ernst & Young
- Sir Ian Prosser, Audit Committee Chair, BP
- Mr Pierre Rodocanachi, Audit Committee Member, Vivendi
- Mr Gerhard Schulmeyer, Audit Committee Chair, Zurich Financial Services
- Lord Sharman of Redlynch, Audit Committee Chair, ABN-AMRO

Members who participated in individual discussions before the meeting were:

- Mr Anders Nyrén, Audit Committee Chair, Skanska and Sandvik
- Dr Klaus Schlede, Audit Committee Chair, Lufthansa and Deutsche Telekom

<sup>1</sup> See European Audit Committee Leadership Network: “Major Emerging Markets Risk”, *ViewPoints*, 30 May 2006. Available at [http://www.tapestrynetworks.com/documents/Tapestry\\_EY\\_Euro\\_ACLN\\_May06\\_View9.pdf](http://www.tapestrynetworks.com/documents/Tapestry_EY_Euro_ACLN_May06_View9.pdf)

<sup>2</sup> “The place of IT Governance in the Enterprise Governance”, Institut de la Gouvernance des Systèmes d'Information, 2005. Available at [http://www.itgi-france.com/content/pub/livrables/place\\_IT\\_governance\\_in\\_enterprise\\_governance.pdf](http://www.itgi-france.com/content/pub/livrables/place_IT_governance_in_enterprise_governance.pdf)

- Dr Ronaldo Schmitz, Audit Committee Chair, GlaxoSmithKline

*ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments made before and during meetings are not attributed to individuals or corporations. Comments described as being provided before the meeting were drawn from discussions with all those listed above.

## Executive summary

IT governance is moving up the corporate agenda propelled by several trends including the increasing cost and complexity of IT systems, the scale and growth of internet-enabled businesses, reliance on vendor IT (whether outsourced or not), the need for IT-related compliance and the increasing risk of cyber-attacks from outside the enterprise.

- **Five key IT risks** (Page 2)

Many members report that their companies address IT risks and opportunities within a broader business context. Enterprise-wide risk mapping is used to identify IT risks. The most commonly cited IT-related risks were identified as: (1) compliance and controls; (2) business continuity; (3) security risk; (4) project delivery and complexity; (5) risks associated with outsourcing.

- **IT oversight by the board and audit committee** (Page 5)

Members agree that there is no 'one size fits all' model for board oversight of IT, which depends more on the nature of the industry and the business model of the company, than on national characteristics. Members revealed a diversity of approach; from boards and audit committees who do not look at IT issues or ever meet with the company's chief information officer (CIO), to those where there is regular oversight of IT risk. European SEC registrants report that focus on IT-based internal controls, during compliance with Sarbanes-Oxley Section 404, is pushing IT onto the audit committee agenda. [For items covered by a CIO reporting twice-yearly to the audit committee of a European SEC registrant, see page 6.](#)

- **Sources of expertise for the board and audit committee** (Page 7)

Members discussed the pros and cons of having independent directors with IT expertise on the board. Several alternative approaches were also discussed, including bringing best practice research to the board, bringing experts into particular board meetings, or setting up a separate advisory board. For audit committees that have oversight of IT risk, the internal and external auditors most often provide the required expertise.

## Five key IT risks

Many members report that their companies address IT risks and opportunities within a broader business context – the application of IT in driving the business forward. IT risks are often discussed by the board without an IT label attached to the item: *"We discuss trading platforms, which are a huge investment, and moving to SAP"*. Another member agreed: *"There is no separation [of IT and business issues]. There are no specific IT topics – it is part of everything else we look at"*.

However, another member cautioned against taking this approach, because it may miss an important class of risk: *"We have driven this too far as being a business issue. Companies have gone too far into*

*proprietary software by that decision. The complexity is beyond the comprehension of the people who run it. [This] is an IT issue”.*

### Five key IT-related risks:

- Compliance and controls – can we rely on the integrity of information?
- Business continuity – can we keep the business running?
- Security risk – can we keep the baddies out?
- Project delivery and complexity – do we get value for money from our IT?
- Outsourcing risk – can we rely on our partners and vendors?

## 1. Compliance and controls – can we rely on the integrity of information?

IT reliability is critical to financial reporting. Indeed, many SEC registrants are looking at leveraging Section 404 compliance as a way to eliminate manual controls. Audit chairs in one US audit committee network said they “expect further benefits [from Section 404 compliance] in the future as manual controls become more automated. In addition, many companies may use technology to convert detective controls (which report failures) into preventative controls (which avoid them)”.<sup>3</sup>

One member representing a European SEC registrant said: *“Against my better judgement – I thought Section 404 was a dead cost – in every case there has been some benefit and IT ... has been critical”.* Several members were using ERP systems such as SAP to speed up the standardisation and automation of internal controls. *“We are getting rid of the spreadsheets,”* quipped one member.

Members also discussed the importance of using IT systems to structure behaviour and implement better practices. One member recommended having all subsidiaries and other entities on the same IT platform: *“All financial control IT is on a global standard... It forces discipline into the culture”.* However, another member said companies which: *“thought they’d standardised on one ERP [system], often had 40-50 versions”.* This level of complexity can lead to significant challenges in the organisation’s control environment.

## 2. Business continuity – can we keep the business running?

In the words of one audit chair: *“Business continuity is critical”.* Several IT experts who were consulted before the meeting recommended questions for the audit committee to ask management:

- What is the plan for significant business interruption?
- What kinds of interruption are we prepared for?
- When did you last test this? What didn’t work?
- What volume can we put through the back up systems?
- What level of redundancy is required and at what cost?
- How long will recovery take?
- Is this auditable?

---

<sup>3</sup> Pacific Southwest Audit Committee Network: “Section 404: year two and beyond”, 29 March 2006, page 2. Available at [http://www.tapestrynetworks.com/documents/Tapestry\\_EY\\_PacSouthwest\\_ACN\\_March06\\_View.pdf](http://www.tapestrynetworks.com/documents/Tapestry_EY_PacSouthwest_ACN_March06_View.pdf)

Prior to the meeting, a CIO of a Fortune 50 company commented: “How much are [companies] assuming the public infrastructure will be there and how long can you wait for it? Assured communications weren’t there for [Hurricane] Katrina or 9/11. If we had depended on public infrastructure, we would have waited two to three weeks for support from the government”. He also suggested audit committees ask about plans for employee recovery –, asking: “where will employees come from to do the recovery work?”.

### **3. Security risk – can we keep the baddies out?**

One member warned about the danger of *“hackers joining forces with criminals... Cyber-crime is an explosive danger for IT”*. Another recommended conducting background checks for employees in the IT department. For one European SEC registrant, the audit chair said that, from a security perspective: *“Section 404 has helped sharpen controls in the IT department”*. There is also a cost and risk trade-off between fixing vulnerabilities in IT systems now and waiting for regular update maintenance later.

The CIO mentioned above suggested the key questions audit chairs should be asking management:

- Would you know if your network had been violated? Does management know what to look for?
- At what level, and with what degree of sophistication, are you monitoring for violations?
- Have you employed third parties to attack the company? What has been changed as a result?

A member suggested asking if the company is using “ethical hacking” by former members of police forces, the military and intelligence agencies, or whether they are using ‘former’ criminals – another risk for the company.

### **4. Project delivery and complexity – do we get value for money from our IT?**

An IT expert commenting in advance of the meeting said: “most large companies see IT spend as their third largest expenditure [measured] as a percentage of operational and capital expenses – the board or audit committee should have a view of value for money. But boards rarely get as involved with IT failures, as they would if it was a factory failure”. Additional issues include cost and cost accounting, timing, project management and implementation of IT projects. One member said, *“Getting down from 100 ERP systems to ten requires you to change everything you are doing”*.

Questions for the audit committee include the following:

- Do we understand the IT strategy and how investments are made?
- Do we understand the impact on shareholder value and share price?
- Is our IT platform conducive to growth and change?

Members are concerned at levels of IT complexity in their organisations. One audit chair commented that companies often fail to standardise business practice before seeking IT support. *“We should say we will only allow a certain amount of complexity: how many systems can we have?”*.

### **5. Outsourcing risk – can we rely on our partners and vendors?**

Members point out that outsourcing is primarily a business risk, not just a technology risk. Due diligence is critical as are very specific service level agreements. Several members had insisted on IT and the internal auditors conducting an audit of IT suppliers before any outsourcing contract was signed.

They also insist on regular audits from their own internal auditors thereafter. Some audit committees are also involved in reviewing SAS 70 reports.<sup>4</sup> In one company, “*All transaction processes are outsourced and the external auditor does a full audit of that*”.

Companies also need to understand the risks associated with linking their suppliers and their customers through the company’s IT systems, regardless of whether the systems themselves are outsourced. As one member commented: “*In the extended enterprise, you give access to people, [in supplier and partner companies], who don’t share your culture*”.

## IT oversight by the board and audit committee

### Role of the board

Members broadly agree with writers of a recent article in the *Harvard Business Review* who said: “There is no one-size fits all model for board supervision of a company’s IT operations. The correct IT approach depends on a host of factors, including a company’s history, industry, competitive situation, financial position, and quality of IT management”.<sup>5</sup>

Approaches to IT governance seem to depend more on the nature of the industry (banks and airlines are more dependent on centralised IT) and the business model (how decentralised or web-dependent) than on national characteristics.

Members revealed a diversity of approach to board oversight:

- **No board discussion of IT.** For some members, the idea of a separate and distinct board discussion of IT strategy does not make sense because technology is integral to the overall business strategy. One member said: “*There is very little exposure to IT or the CIO... IT is a tool like any other and the controls on IT are the same as those for manufacturing tools*”.
- **Regular discussion of IT.** Some members felt very strongly that IT is a board matter. One audit chair said: “*How can I sit and spend time on a nitty-gritty accounting issue when, on the IT side, I can see things that will blow us away?*”. Several members said their boards reviewed IT once or twice a year, with a report from the chief information officer (CIO) on how IT functions, decision-making process, policy setting, budgets and authorisation levels and alignment with strategy and business process. In other cases, it is the audit committee chair or the CEO who gives the IT report to the board.

### Role of the audit committee

The governance codes of the countries represented by network members do not provide much clarity on the role of the audit committee in IT oversight, except in one case.<sup>6</sup> While there is broad agreement among members that the degree of board involvement in IT depends on the industry and the business model, there is disagreement about the role of the audit committee, varying from none at all, to

<sup>4</sup> The American Institute of Certified Public Accountants’ Statement on Auditing Standards No. 70, Service Organizations (SAS 70), contains the professional standards for auditors to report on the controls of a service organisation. For more information, [http://www.ey.com/global/content.nsf/US/AABS\\_-\\_TSRS\\_-\\_Services\\_-\\_SAS\\_70](http://www.ey.com/global/content.nsf/US/AABS_-_TSRS_-_Services_-_SAS_70)

<sup>5</sup> Richard Nolan and F. Warren McFarlan: “Information Technology and the Board of Directors”, *Harvard Business Review*, October 2005.

<sup>6</sup> The Dutch code states: “The audit committee shall in any event focus on supervising the activities of the management board with respect to ... the applications of information and communication technology (ICT).” Section III.5.4 (h) of the Dutch corporate governance code: Principles of good corporate governance and best practice provisions, Corporate Governance Committee, 9 December 2003, page 21.

assessment of IT role in internal controls – *“IT goes to the audit committee via the internal audit function that oversees all systems and ensures controls are built in”* – to complete oversight of IT risk along with other risks facing the company.

Commenting on the latter role, one member said: *“We look at all types of risk, including operational risk. In addition, some [IT] deficiencies have been found by internal audit or the external auditor”*. Another member said: *“The audit committee reviewed the process by which the company dealt with ... [technology] risks and then reported to the board. The audit committee did the detailed work”*.

#### **Examples of items covered by a CIO reporting twice-yearly to the audit committee of a European SEC registrant:**

- **IT strategy**
- **Business continuity**
- **Access hierarchies**
- **Control deficiencies identified by internal audit**
- **Post-acquisition IT integration**
- **Reviews of SAS 70 reports on outsource vendors**

### **Role of the CIO**

Members had mixed views about the need for and role of the CIO. For many European companies, this role does not exist at group or holding company level: *“We have no CIO and no role for one”*. Another member joked: *“There’s no head of strategy. It doesn’t mean that strategy is not important”*.

Where there is a CIO role, the typical reporting line in many mainland European companies is through the finance director. In these cases, the CIO rarely reports to the board directly unless there is a problem. A number of members reported that they have never met their CIO. One member said his CIO will be participating in an upcoming audit committee meeting and this will be the *“first time I have met this officer”*.

By contrast, where IT is central to the business strategy, the CIO often reports directly to the CEO. In these cases, there is board and audit committee contact. One member said: *“CIOs know more than they can explain”* and often need help packaging what they know for the audit committee so they can *“address concerns without scaring people”*.

Another member said that the operating units in a company need to be good buyers of IT and that a CIO can help them. One audit chair recommended: *“Get the software writers out of the company and get a CIO instead”*. He believes that software developers often add to complexity, while good CIOs can create common standards and infrastructure for the company.

This situation is supported by research published in *InSights* in the US last year: “[T]here appears to be a link between the company’s management reporting structure and the presence of a direct relationship between the CIO and the audit committee. Every CIO who reports directly to the chief executive

officer presented directly to the audit committee. In contrast, if the CIO reports to the chief financial officer or to another individual..., direct contact with the audit committee was unlikely to occur”.<sup>7</sup>

## Sources of expertise and education for the board and audit committee

### Expertise and the board

According to a survey by Burson-Marsteller, in 2004 only 8% of Fortune Global 500 companies had a current or former CIO on the board.<sup>8</sup> A couple of members said the lack of such expertise is one reason their boards do not currently discuss IT. One member speaking before the meeting remarked: *“When you dig in, it’s a black hole for most top management and boards”*.

Those members who favoured having IT expertise amongst the board directors felt that former or sitting CIOs who could bring a strategic view of the business impact of technology were highly valuable. However, one member disagreed saying: *“A CIO is not the best expert on IT. Real experts are scientists or research people. The CIO is an operating officer”*.

However, an article in *Corporate Board Member* suggested: *“The task of IT oversight isn’t unduly complex. Board members need not be technology experts, nor should they try to micromanage technology initiatives. As in financial or other strategic matters, however, directors are expected to understand the big-picture strategy and ask intelligent questions about how technology fits into it”*.<sup>9</sup>

Several alternatives to having an expert director on the board were also suggested by members:

- **Bring best practice research to the board.** One member suggested that, at the very least, boards could insist on receiving reports on best practice. For instance, assessing compliance with COBIT,<sup>10</sup> a framework designed to identify common IT risks.
- **Bring experts into particular board meetings.** *“Invite them to a strategic away day... I’m not sure that having a CIO on the board is important. Boards need free thinkers [on strategy].”*
- **Set up an advisory board.** Several members advocated the idea of a special advisory board for the company. One member said: *“An advisory board could be helpful for some companies to understand these matters. You need so much discussion [that] the board is the wrong level”*.

### Expertise and the audit committee

If the audit committee plays a role in the oversight of IT, it needs access to expertise at its meetings. As one member pointed out: *“Most people on the audit committee didn’t grow up with computers”*. Speaking before the meeting another member said: *“It is important to have someone on the audit committee who knows about information and information handling”*.

<sup>7</sup> *InSights*: “The CIO’s perspective”, 28 February 2005, page 6. Available at [http://www.tapestrynetworks.com/documents/Tapestry\\_EY\\_ACLN\\_Feb05\\_InSights.pdf](http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Feb05_InSights.pdf)

<sup>8</sup> “A Missing Competency: Boardroom IT-deficit”, Burson-Marsteller, 2005, page 6. Available at [http://www.burson-marsteller.com/pdf/IT\\_Deficit\\_2005\\_Brochure.pdf](http://www.burson-marsteller.com/pdf/IT_Deficit_2005_Brochure.pdf)

<sup>9</sup> John R. Engen: “The New Challenge for Directors”, *Corporate Board Member*, May-June 2006. Available at [http://boardmember.com/issues/archive.pl?article\\_id=12467&V=1](http://boardmember.com/issues/archive.pl?article_id=12467&V=1)

<sup>10</sup> COBIT stands for Control Objectives for Information and related Technology.

Sources of expertise for the audit committee include:

- **Internal audit.** Internal audit is a key source of IT expertise for the audit committee and a number of member companies had invested in upgrading the technology skill set of the function. However, one member cautioned that internal audit cannot always attract the right calibre of IT talent, almost irrespective of the level of investment: *“Are the internal audit people good enough? Are the salaries high enough to attract good IT people?”* Another member responded: *“You get the internal audit function you deserve. We have IT people on rotation in the function”*. Another option is to co-source IT specialists with the Big Four accounting firms.
- **External auditor.** Audit teams include IT experts who focus on the complexity and risk of applications. One member said before the meeting: *“We rely on the external auditor to do an audit of IT controls and security”*. An IT expert talking before the meeting estimated that 15-25% of audit hours are IT-related. The audit firms are building expertise in all major IT systems and are developing tools to address control aspects of these IT systems. For SEC registrants, the external auditor is also involved in probing and testing IT controls as part of their Section 404 attestation. Members felt the auditor should be able to present on IT risks and the impact of the regulation.
- **Other third parties.** Members identified management consultants and systems integrators as sources of advice. One member said: *“We looked for technical expertise beyond the external auditor. There are other good [sources] around”*.

## Conclusion

After the first five meetings of the network, a pattern appeared in how members thought about the role of the audit committee. Their perspectives were shaped primarily by national history, cultures, laws and regulations and emerging EU regulations. The result: a range of audit committee models on a spectrum from active committees that had oversight of all enterprise risk, to those committees that had no involvement in governance beyond financial reporting.

When considering IT governance, while the same spectrum exists, the reasons are quite different and are based instead on the nature of the enterprise, the industry in which it operates, and its business model. However, a focus on internal controls, whether driven by the need to comply with Sarbanes-Oxley Section 404 or not, is slowly pushing European audit committees into greater consideration of IT issues – at least as they impact financial reporting.

## About this document

The European Audit Committee Leadership Network is a select group of audit committee chairs from leading European companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is convened by Ernst & Young and orchestrated by Tapestry Networks to access emerging best practices and share insights into issues that dominate the new audit environment.

*ViewPoints* is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, their advisers and auditors, as they endeavour to fulfil their respective responsibilities to the investing public. *ViewPoints* is a synthesis of key issues arising from discussions among members of the European Audit Committee Leadership Network. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Anyone who receives *ViewPoints* may share it with those in their own network. The more board members, management, advisers and auditors who become systematically engaged in this dialogue, the more value will be created for all.

*The views expressed in this document represent those of the European Audit Committee Leadership Network, a select group of audit committee chairs from Europe's leading companies committed to improving the performance of audit committees and enhancing trust in financial markets. They do not reflect the views nor constitute the advice of network members, their companies, Ernst & Young or Tapestry Networks. Please consult your advisers for specific advice. Ernst & Young refers to all members of the global Ernst & Young organisation.*

*This material is copyright Ernst & Young and prepared by Tapestry Networks. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends.*