EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING

ECIIA

THE FUTURE OF CORPORATE GOVERNANCE

KEY VIEWS FROM KEY PEOPLE

ENHANCING GOVERNANCE THROUGH INTERNAL AUDIT

INTRODUCTION

While Europe is still feeling the effects of the economic and financial crises of 2007 - 2008, from a corporate governance perspective it has started to move on.

The European Commission has been busy restructuring the rules and guidelines under which business will be done in the region for the next generation. The main policy reforms to the financial sector and to company law and corporate governance are in progress and there is still work to be done.

As we move forward, it is worth remembering that corporate governance is only one part of the solution to the problem of creating wealth in a more sustainable way. For that to happen, businesses must be more transparent, bring independence to their assurance and communicate clearly with their broader stakeholders. It is within that context that the Three Lines of Defence model of corporate governance can be of great help and that the role of internal audit is key.

We wanted to ask those representing core participants in the corporate governance system whether they were happy with the direction the changes had taken. How well would the reforms achieve their objectives? We wanted to hear about the role of internal auditors in the future of governance. How could they help organisations manage their risks and create value?

The result of our curiosity is this booklet. It represents a snap shot of views at the very time when organisations are getting ready for the new corporate governance landscape.

In the opening interview, Ugo Bassi, the Director in the European Commission's Internal Market DG in charge of Capital and Companies Directorate, explains that the guiding principle to all of its reforms has been the concept of transparency. This has allowed it, he believes, to strike the right balance between better disclosure and risk management on the one hand, and over-prescriptive rules on the other.

While the other participants in the project voice reservations on specific details to the reforms, all are agreed that the Commission has listened and adopted the right approach – that Europe's corporate governance system will be more robust and better able to cope with crisis in the future. Under the new regime, internal audit is likely to play a larger, more pro-active role in providing assurance to the board that its risks are identified and well managed, and that its controls are in place and functioning properly.

It remains for me to thank the participants Ugo Bassi, of the European Commission, Patrick Zurstrassen, Chairman of the European Confederation of Directors' Associations, Carlos Montalvo, Executive Director of the European Insurance and Occupational Pensions Authority, Michel Dennery, Vice President of the Federation of European Risk Management Associations, and Armand Lumens, Head of Internal Audit at the energy group Shell.

Marie-Hélène Laimay
ECIIA President

CONTENTS

TRANSPARENCY IS THE KEY

The European Commission's reform of the region's Corporate Governance regime is based on the guiding principle of greater transparency, according to Ugo Bassi, Director in the European Commission's Internal Market DG in charge of the Capital and Companies Directorate

"In our view, corporate governance should contribute to long-term sustainable growth – and be a win-win game," says Ugo Bassi, the Director in the European Commission's Internal Market DG in charge of the Capital and Companies Directorate. "Society benefits from high-performing companies and the companies benefit from a good environment that facilitates growth."

He is in no doubt that poor corporate governance in financial institutions contributed to the financial crisis of 2008 and that traditional systems of checks and balances failed to work properly in at least two major areas: risk management and shareholder stewardship.

> "We would like to inject as much transparency as we can into the system"

In risk management, for example, he argues that prior to the crisis a board would have often failed to receive sufficient information to correctly assess the risks that it wanted to take.

"We are not saying boards were not equipped to take risk management decisions, or that they were unable to do it because of poor decision-making processes," he says. "What we saw is rather that the level of information and awareness of its importance was often not sufficient."

Risk management, he says, was also too focused on assessing risks in the individual silos of the business and often failed to take a view of the whole enterprise, which made the situation worse: "It is very difficult to have an overview of the total level of risk and how different risks interact if the risk assessment is activity-based," he says.

These failings, and the reasons behind them, have informed much of the Commission's thinking on its reforms both in the Capital Requirements Directive and in the European Union's subsequent Company Law and Corporate Governance Action Plan.

If there is a single word that captures the Commission's approach to finding a solution to these issues for listed companies, it is transparency, which Bassi calls the key word.

"We would like to inject as much transparency as we can into the system," he says.

This strategy has enabled the Commission to move away from prescribing hard and fast rules that would have been unpopular in much of the business community. In addition, it has ensured that reforms have remained sensitive to the different national cultures, traditions, regimes and codes of conduct existing in Europe's 28 Member States.

Bassi points to three recent areas of reform in which transparency has acted as a guiding principle: the current proposals on ▶

▶ board diversity and the management of non-financial risks, the adoption of the "comply or explain" principle in reporting, and moves to improve shareholder engagement.

With the first, he says that instead of imposing specific targets on, for example, the composition of boards, the Commission wants to make companies report on their policy objectives and to disclose better information. "By obliging companies, on a comply or explain basis, to report and disclose information about those policies, they will be encouraged to decide what are in their specific situation the right and the most appropriate objectives," he says.

Similarly, he expects the "comply or explain" principle to inject further transparency into the corporate governance system. He hopes that companies will embrace the spirit of the principle and explain, not why they do not comply with their national codes, but how they achieve similar results and objectives by other means while defining clear time limits. The aim would be to provide Member States with guidance on how the principle of "comply or explain" should be applied consistently throughout Europe while leaving companies to choose their own solutions to their corporate governance challenges.

Finally, he believes that providing greater transparency on company policies and behaviour to shareholders will encourage them to actively engage with the businesses in which they invest. For example, shareholders could be given power to vote on directors' remuneration policies. But he admits that this is a challenge: "The more the shareholder knows, the more he will be involved in the life of the company," he says.

The Commission has not drawn any specific conclusions on revising the role of internal audit to date, he says, noting that improvements in risk management practice imply a strengthening of internal audit's role. But while the Action Plan has a long way to go before its provisions are in place, the Commission is already looking to the future and that could mean more reform. "We see the Action Plan as a first round of measures," he says. "There are a number of other measures, which are not included in the Action Plan, which are being studied at the moment."

While that may dismay some, Bassi ultimately hopes to create a wide-ranging change in corporate governance culture that will be of lasting benefit to European society. A culture that is more open and focused on sustainability. "I think that when we have improved the functioning of the board, enhanced and improved the quality of engagement of shareholders, we will be heading towards our final objective – which is a culture of more sustainable and long-term growth," he says.

> **"Providing greater transparency on company policies and behaviour to shareholders will encourage them to actively engage with the businesses in which they invest"**

CENTRE STAGE FOR SOCIAL RESPONSIBILITY

Reforms have helped stakeholders make clearer comparisons between companies in both their financial and social performance, says Patrick Zurstrassen, Chairman of the European Confederation of Directors' Associations

"The general responsibility adopted by a board of directors is not only towards the company and its shareholders, but, in a broader sense, to its stakeholders too," says Patrick Zurstrassen, chairman at the European Confederation of Directors' Associations (ECODA). While some dispute this view, he believes that the evidence points to stronger links between corporate governance and social responsibility in many European companies.

"This shift can be seen most obviously in the way that non-financial reporting is growing considerably in corporate governance practice," he says. Companies are providing more information about the impact of their work in areas such as the environment, their involvement with local communities and on issues such as gender equality among staff. None of this information was the subject of public disclosure twenty years ago for most businesses.

Even so, the trend is still in its infancy, he says. He wants to see more work done on understanding the nature and role of non-financial reporting, for example, and on what forms of measurement might be appropriate for the board. But he says the overall goal is for businesses to make the link between their behavior and its social significance clear.

> "The comply or explain practice accommodates the wide diversity of business models operating across the many legal jurisdictions that make up the European Union"

"We are looking for greater transparency so that companies can be compared, not only on financial terms, on the stock price, but also on the contribution that the organisation is making to society," he says.

Businesses are increasingly placing emphasis on the role of audit committees and internal audit within their corporate governance structures, ▶

▶ he says. “More and more organisations have audit committees,” he says, “and you cannot have an audit committee in abstraction. You have to have an audit committee with a budget, with a plan, with resources, and that is provided by internal audit. If the audit committee wants to be effective, it has to organise in a formal manner the relationship with the internal audit function.”

He says that the Three Lines of Defence model has played an important role in clarifying how best to structure the relationship between a business and its internal audit function. This has led to better scrutiny of both issues of social responsibility and to areas such as the quality of the work of external audit and other suppliers, he believes.

These trends are likely to be further strengthened by the approach taken to the reform of corporate governance by the European Union’s Action Plan. One of his concerns in the lead up to the publication of the Plan was that the Commission would adopt a rule-based approach that would lay down a set of prescribed behaviours for all businesses in the European Union. But he says he was delighted when it announced that it had chosen to stress the importance of the “comply or explain” model of disclosure, which was first pioneered in the United Kingdom in the early 1990s. Under this regime, companies follow principles laid down in the corporate governance codes of their national countries, or explain in their annual reports why they have decided not to do so.

The “comply or explain” practice, he says, accommodates the wide diversity of business models operating across the many legal jurisdictions that make up the European Union. It allows for one-tier, or two-tier corporate governance systems; nomination processes that are different; a variety of relationship styles between the shareholder assembly and the board and management; the presence or absence of labour representatives on the board, and many other ways of working that would have disappeared under a single system of corporate governance rules.

He admits that the implementation of this model is still a work in progress, with better monitoring needed on the quality of explanations and the comparability of statements in annual reports. But he regrets that the European Commission has drawn away from the spirit of this overall approach in some areas – such as gender equality and the number of boards directors are permitted to sit on – where, he says, it is shifting to hard rules with inflexible limits.

He believes that the model of corporate governance was still in its infancy when the financial crisis hit Europe in 2008. A whole range of reforms has strengthened it since. While that does not guarantee a trouble-free future, it has given him confidence that corporate governance is going in the right direction.

> **“If the audit committee wants to be effective, it has to organise in a formal manner with the internal audit function”**

RISK-BASED APPROACH FOR INSURERS

The risk-based governance framework the European Commission has designed for insurers should put businesses on a firmer long-term footing, provided they do not treat it as a compliance exercise, says Carlos Montalvo, Executive Director of the European Insurance and Occupational Pensions Authority

"Governance needs to set the right structure within a company to facilitate decision making and running the business," says Carlos Montalvo, Executive Director of the European Insurance and Occupational Pensions Authority. He believes that prior to the financial crisis of 2008, European businesses in the insurance sector and beyond often had a poor grasp of the potential benefits of sound corporate governance.

"Too many organisations saw governance as just a number of compliance requirements," he says, "rather than as providing those essential elements to the board that facilitate good decision making."

He says businesses often lacked the right incentives to pursue sustainable growth, and suffered from an absence of sound and timely information, although this was partly mitigated in the insurance sector because of its focus on traditional core business. In addition, there was little convergence among European Member States in their approach to corporate governance, which may have added to the impact of the crisis across the zone.

> "There is a danger that companies will continue to regard Solvency II as a mere compliance exercise"

The European Union is seeking to address some of these issues through the Solvency II Directive, which aims to codify and harmonize EU insurance regulation.

Montalvo says that the Directive addresses the shortcomings uncovered during the financial crisis by adopting a risk-based framework. It aims to give the same relevance to all the three pillars of the business – defined under Solvency II as quantitative requirements, supervisor review and market discipline: it offers better guidance on how much capital insurers must hold to reduce their risk of insolvency. This is particularly useful for insurers because it provides a clear and explicit link between risk management and systems of governance – making each central to the business. Finally, he says, the Directive boosts the quality and timeliness of information to the board and to supervisors, embedding transparency and disclosure into the fabric of the company.

But the success of the Directive needs a change in mindset. Montalvo says that there is a danger that companies will continue to regard Solvency II as a mere compliance exercise, and miss the business benefits that embracing the new regime could bring. He also worries that regulators may see the requirements of the Directive as immutable and force companies to take a rigid approach to enacting its provisions.

"There is a danger that supervisors could treat Solvency II as a straight-jacket from ►

▶ which businesses cannot move," he says. "But companies across Europe have very different realities, so they should be permitted to adopt requirements depending on their own situations based on the principle of proportionality that we have in Solvency II."

While he believes internal audit has a role to play within Solvency II, he says that the function's remit goes beyond the Directive: "As a manager, I see internal audit as a service that is able to identify both weaknesses and strengths in my institution. It can provide me with ways to improve on those weaknesses, and empower me to build on my strengths."

> **"I see internal audit as a service that is able to identify both weaknesses and strengths in my institution"**

He sees internal audit as a constructive function that is able to generate and add value to the organisation. This can be seen, for example, in the way that a chief audit executive follows up on audit recommendations. "They can locate the responsibility for improvement and say, 'well, this is an area we need to work upon – let's do it.'" He believes that the perception of internal audit is changing and managers are increasingly seeing the benefit of its work to their part of the business, rather than perceiving it as an unwelcome imposition.

Solvency II significantly reinforces the focus on systems of governance, risk management, internal control frameworks and the actuarial function – grouped together under the Directive as qualitative requirements for the business. While that gives internal audit a better voice and platform in the organisation to make its recommendations, Montalvo says that to make the most out of this position, internal auditors need to better understand the realities and needs of the business in order not to be perceived as "aliens" by the rest of the company.

"Internal audit could contribute to a better understanding of the risks within the company," he says, "but it should concentrate not only on gaps, but on strengths too." He would like to see more functions helping management share best practice across the organisation.

"You don't need to neglect the traditional internal audit work of identifying weaknesses and gaps," he says, "But when you look at things that work in a company, you try to understand why that is the case. Ask, 'how can I share and spread that element that is working well within one part of the company to other areas of that business?'"

Montalvo cannot guarantee that Solvency II will make the Eurozone immune from future crises. But he is optimistic about the type of risk-based framework the Directive outlines.

"What is also positive and good in a risk based system is that ideally it will provide you with sufficient information that can dissipate some of the effects and consequences of a future crisis. It enables you to take some pre-emptive measures and therefore lessen the effect; pre-empting is, by definition, cheaper and more efficient than fixing" he says.

LOOKING TO THE FUTURE

The reforms have placed a heavy emphasis on better, more forward-looking risk management practices, says Michel Dennery, Vice President of Federation of European Risk Management Associations

"Corporate governance can be seen as a system composed of ethics on the top, then risk management, internal control and internal audit," says Michel Dennery, Vice President of Federation of European Risk Management Associations (FERMA). "We cannot lead a company without ethical values. It contributes to the identity and personality of the company and it informs the way it behaves vis-à-vis stakeholders."

Back in 2007, just before the financial crisis hit Europe, he believes that the focus on ethics had slipped down the agenda. People were acting in something close to a virtual economy that had its eyes set firmly on a future of perpetual growth.

The warning signs – what he calls "signaux faibles" – were evident, but generally ignored. They included the fact that leading economists were pondering whether the world's large economic zones would falter if one of them were to fail; the widespread practice of tritrization, in which companies slew off risky debt into bond-financed companies; and, the equally widespread use of leveraging balance sheets in the belief that economic growth would reduce the value of debt.

> **"One of the main lessons of the 2008 crisis is that risk management has been listened to much more by management"**

Given Dennery's belief that risk management's job is to look to the future, how did businesses allow themselves to get into such risky positions?

"At that time, risk management was still a young function in companies," he says. "It was difficult for risk managers to be heard by top management. One of the main lessons of the 2008 crisis is that risk management has been listened to much more by management."

Corporate governance reforms have brought in positive changes, he says. The 8th Company Law Directive, Solvency II, and Basel III have greatly strengthened the influence of European risk managers in different ways.

The 8th Directive, for example, says that the audit committee and the board directors must monitor risk management. This has placed responsibility for risk taking directly onto the shoulders of board members. "They have to question management about risk appetite and, of course, these responsibilities cascade through the organisation," he says.

Basel III has compelled banks and financial institutions to improve their balance sheets and has made them more prudent about taking risks and financing business. And Solvency II is likely to introduce what Dennery calls the "retro-transfer" of risk. When it comes into force, insurers will need to be clear how much capital is at risk for each contract. Thus, to reduce this capital at risk, they may encourage companies to improve their reduction plans.

"The client will have to prove that it has a very good level of risk management, and that the risk is really limited to what is supposed to be transferred," he says. While that may increase exclusions, it should force companies to improve their risk management processes.

But he does not support a more prescriptive model of corporate governance than what has already been outlined in the ►

▶ European Union Action Plan and would not favour detailed regulation. He even worries that the European Commission's drive towards transparency could go too far and threaten the competitive advantage of European business.

"Being more and more transparent is not a guarantee of preventing fraud, bad behavior, or corruption," he says. "Promoting an ethical code of conduct in the company, and a strong involvement of the CEO are much more efficient."

In fact, he says, the Three Lines of Defence model of corporate governance, comprising risk management, internal controls and internal audit, can greatly enhance the effectiveness of risk management and board oversight.

Risk management's role is to identify and assess risks and this feeds into the audit plan, he says, or it can help set the priorities for critical internal controls. But it may use issues that emerge from internal audit to improve its own assessments. In addition, internal audit assesses how internal control contributes to controlling the day-to-day risk in the business. "The synergies between the three activities can be very well organised," he says.

Overall, he believes that the architects of Europe's new corporate governance regime have made a very positive step. The region still remains vulnerable to external shocks, and he worries that the current focus on prudence may inhibit growth in Europe – thereby prolonging the effects of the crisis. "Risk management should be considered as a strong support for sustainable development in empowering decision making and risk taking," he says.

ENHANCING CORPORATE GOVERNANCE THROUGH INTERNAL AUDIT

The European Commission says that strengthening risk management implies a greater emphasis on internal audit. Armand Lumens, Head of Internal Audit, Shell explains how to get the most from an internal audit function

"The primary purpose of internal audit is to provide assurance on the company's control frameworks," says Armand Lumens, Head of Internal Audit at the energy and petrochemicals group Shell. Internal audit gives this assurance to different levels of the company including to the management teams, the executive directors, the audit committee and to the board.

"I personally connect with all of those levels in the company every quarter," he says. "On top of that, I have direct conversations with the chief finance officer and the chief executive officer of the company on a periodic basis." The company has an overall control framework, as does every business and every aspect of each project in the company.

"Internal audit assists in risk management and holds a mirror up to the company," he says. As well as conducting audits, writing reports and making recommendations, internal audit helps the lines of business to manage their risks better.

"We have a teaching function in the business to explain that we are about risk management and that eventually we want the business to manage its own risks and not use audit every ▶

▶ time to tell them what is wrong," he says. "This is a part of integrated risk management that is extremely important because education on risk management leads to proper governance."

"Internal audit gives insights on the strengths and weaknesses in the business to the audit committee and to the board," he says.

"There is always a risk in a company that what really happens on the ground is watered down and that different messages reach the top," he says. Internal audit's independent status enables the function to bring information to the board and the executive committee without filters. That helps decision-makers to discuss the real issues at the right level of the business.

"Internal audit makes sure the business clearly understands what the various levels of its defenses are," he says.

Lumens subscribes to the Three Lines of Defence model of corporate governance promoted by the ECIIA. In that system, the first line of defence includes business controls, IT controls, contracts and other business processes; the second includes the business line's own review of its control mechanisms; and the third is internal audit, which is the independent layer that checks whether the business self-assurances are right and well set up.

"Three Lines of Defence is a neat way of explaining that management is in control of its destiny, its risks and the business," he says. "It also helps explain who is responsible for what in terms of risk management."

Shell is a global group of energy and petrochemical companies with around 90,000 employees in more than 80 territories. The audit function comprises over 220 people, with 35 different skill sets, based in 9 locations globally. Over 90% of audits are on non-financial issues.

"Three Lines of Defence is a neat way of explaining that management is in control of its destiny, its risks and the business"

OUR MISSION

To be the consolidated voice for the profession of internal auditing in Europe by dealing with the European Union,its Parliament and Commission and any other appropriate institution of influence and to present and develop the internal audit profession and good corporate governance in Europe.

IIA Austria	www.internerevision.at
IIA Azerbaidjan	www.audit.gov.az
IIA Belgium	www.iiabel.be
IIA Bosnia and Herzegovina	www.interni-revizori.info
IIA Bulgaria	www.iiabg.org
IIA Croatia	www.hiir.hr
IIA Cyprus	www.iiacyprus.org.cy
IIA Czech	www.interniaudit.cz
IIA Denmark	www.iia.dk
IIA Estonia	www.theiia.org/chapters
IIA Finland	www.theiia.fi
IIA France	www.ifaci.com
IIA Germany	www.diir.de
IIA Georgia	www.theiia.org/chapters
IIA Greece	www.theiia.org/chapters
IIA Hungary	www.iia.hu
IIA Iceland	www.fie.is
IIA Italy	www.aiiaweb.it
IIA Latvia	www.iai.lv
IIA Lithuania	www.theiia.org/chapters
IIA Luxembourg	www.theiia.org/chapters
IIA Montenegro	www.iircg.co.me
IIA Morocco	www.theiia.org/chapters
IIA Netherlands	www.iia.nl
IIA Norway	www.nirf.org
IIA Poland	www.iia.org.pl
IIA Portugal	www.ipai.pt
IIA Romania	www.aair.ro
IIA Serbia	www.theiia.org/chapters
IIA Slovakia	www.skiia.sk
IIA Slovenia	www.si-revizija.si/iia/
IIA Spain	www.iai.es
IIA Sweden	www.internrevisorerna.se
IIA Switzerland	www.svir.ch
IIA Tunisia	www.iiatunisia.org.tn
IIA Turkey	www.tide.org.tr
IIA UK & Ireland	www.iia.org.uk

European Confederation of Institutes
of Internal Auditing (ECIIA)

Koningsstraat 109-111
Bus 5, BE-1000
Brussels, Belgium

www.eciia.eu

The Institute of Internal Auditors