

Corporate Governance

By Marc Sel – CISA, CISM, PricewaterhouseCoopers – 2004-06

When I took my CISA exam back in 1993, I could not help but having the impression that many looked upon ISACA as just a good source of checklists. Since then, we've surely come a long way. It's a great pleasure to share some points of view on governance with you and fellow members.

Value creation, specialisation and ethics

Value creation takes many forms, and takes place in many different environments. Public and private organisations operate in a mode that can range from a reasonably open democracy to a more dictatorial model, with a range of possibilities in between. Controls are built-in, but occasionally fail, as we've witnessed in the cases of Barings, Enron, GlobalCrossing, WorldCom, Ahold, etc.

Despite the many different ways to create value, it can be stated that within the industrialised world, and particularly in the 21 century, specialisation is the name of the game. Whether you are teaching, managing, researching, selling, or performing any other professional activity, your environment expects you to have a skill-set that contains a significant amount of specialisations. And virtually all environments depend to a large extent on IT. So it is clear that if we strive for a responsible governance model, it should recognize our dependence on IT, and also on specialists (including both IT and non-IT specialists). We will not elaborate on the aspects of trusted IT-hardware (e.g. HSM) in this article but will leave that to another occasion. We prefer to focus on the human specialists. These have to be trusted, and for this reason both a code of ethics and a form of monitoring are key. That's what organisations such as IEEE and ISACA have understood very well. Last year PricewaterhouseCoopers internally communicated a concise and well-written code of ethics for internal use. Our code of ethics embodies our values, in plain language, understandable and sharable by all. Even an IT-techy such as myself could make sense of it. That's what I call a contributor to good corporate governance.

Free agents

Besides the ever-increasing specialisation, we witness an evolution from a model of life-long employment towards a model where people become 'free agents' that make their own choices on where to deploy their talents and energy. While Unions and Syndicates were always an important part of the organisational landscape in the past, they are also constantly confronted with new organisational challenges and globalisation. Unions and Syndicates are and will remain important, but have to adapt to the evolving needs of their members. So if we strive for a responsible governance model, we should search the balance between healthy entrepreneurship, creative energy and protection of the less stronger members of the group. And it's obvious that privacy is a battlefield, both in the setting of the individual and of the organisation. So if we strive for a responsible governance model, addressing privacy concerns should be an integral part of it.

More and more, each individual will decide where to contribute, and exactly what to contribute. Especially in professional environment where specialisation is so important, continuous education is important, and this is inherently a personal matter. So if we strive for a responsible governance model, education should be an integral part of it.

Accountability

One of my most favourite writers once put the question of life as: ‘What have you done to decrease the pain?’ Leaving it to yourself to specify which pain you selected. While the way we chose is clearly a matter of individual taste, the measures society takes as a whole provides also an interesting indication of priorities and trends. In certain cases, watching the television news can lead to the conclusion that some of us are engaged in activities opposed to decreasing pain. Worldwide networks of espionage such as Echelon are a fact of life, but have done little to decrease pain. Starting a war on the basis of incomplete or inaccurate information does not decrease pain either. So if we strive for a responsible governance model, transparency should be an integral part of it. Transparency will allow individuals to inform themselves about what and where to contribute, and under what leadership. But it is wise to hold leaders accountable. So if we strive for a responsible governance model, accountability should be a part of it.

Balanced Scorecard - XXXL

An interesting initiative to measure how well we proceed towards a more acceptable world is the Human Development Index or HDI, published in an annual UN report. The Human Development Report has the ambition to be an independent report. It is commissioned by the United Nations Development Programme (UNDP) and is the product of a team of scholars, development practitioners and members of the Human Development Report Office of UNDP. The Report is translated into more than a dozen languages and launched in more than 100 countries annually. It is going beyond income to assess the level of people’s long-term well-being, looking at education, health and production. In this way, it can be looked upon as a world balanced scorecard. The report’s ranking does not always match our ‘natural’ expectations, but in quite a few cases rather challenges them.

Transparency

In order to be able to define and measure the HDI, we need a certain degree of openness and transparency. However, accepting the fact that not all individuals share the same values and agree on what are acceptable means to make them heard, gives rise to a difficult question. How to balance transparency and openness, with the privacy of the individual or the corporation? Obviously, there is no simple answer to this question, and many wrong answers have already been given in the course of history. In Belgium we are very much used to the fact that there is a central government identity database, that keeps track of important events in life (birth, marriage, children, where you live, etc). We are now gradually rolling out Java-based smartcards as identity cards. In other countries, identity cards are unheard of. Nevertheless, we witness that evolving technology combined to real-world facts sometimes provokes a fundamental change. The United Kingdom had no ID-cards since World War II, but now under political and economical changes, recently 10.000 UK-citizens started to become enrolled in a biometrical smartcard trial. Gradually

this new deployment of technology is being seen as a way to promote a better society, including a fairer distribution of benefits. Obviously any system has a potential for failure and misuse, and good governance is more than appropriate. Should we store gender? Religion? Preferences? Accreditations?

Especially now when there are large scale initiatives to have even a single EU-wide identification mechanism (probably including a relatively immature mechanism such as iris scan), we should ask ourselves these questions. And obviously, the challenge does not stop there. For a moment, assume we have a number of identity-management systems. Assume these are organised on a per-continent basis, and there is a pragmatic approach established with regard to mutual recognition, politically and technically acceptable. Then we've only addressed the authenticity aspect of security. Underneath this surface there's the even more complex problem of authorizations. Especially in a context of governance, authorizations are key. Who can approve or sign what? How do we guarantee segregation of duty on large scale? Across organisational or national boundaries? And just about how much transparency is justifiable (or enforceable) if we take the perspective of value creation under fair terms? I'm sure the challenges for adequate corporate governance are only starting to become apparent.

Summing up

So if we turn towards corporate governance, and look at how value is created and how organisations are engaged in business, we cannot fail to observe that good governance is essentially a call for responsible action. So what we are looking forward to is action. What's your next move?

Marc Sel

Is a director with PricewaterhouseCoopers risk management practice in Belgium. He holds a Master in Information Security from Royal Holloway University of London, as well as a CISA and a CISM certification. He joined Coopers & Lybrand in 1989 as a Management Consultant, and evolved into the security advisory field. He can be contacted via marc.sel@pwc.be