

Is integration of the various management systems entities use the response to sustainable competitiveness in an increasingly regulated global business place?

A conference held in Philadelphia on September 17-18, 2005 under the auspices of the American Society for Quality (ASQ) seems to support that view.

By Alain Gaumier and Mariann Zanardo< CHMM.

Summary:

- Sarbanes-Oxley projects have proven to be costly for American companies. There must be a better use of their resources. This is one of the benefits of integrating management systems.
- Balanced scorecards and the 2005 Baldrige criteria are tools that already support such integration. However they do not reinforce the United Nations definition of sustainability.
- Companies are facing compliance requirements to a lot of regulations globally. Financial and environmental perspectives are already connected through the SEC disclosure requirement.
- ISO standards can bring to SOX proven processes that sustain the required internal controls, such as the experience of a controlled documentation system. The SOX projects can also be used to strengthen the QMS and EMS of an organization, like the use of the CobiT framework to set up solid IT internal controls.
- Some companies have already embarked on the integration of their management systems, and were represented at the conference. One of the various possible approaches is to first integrate the internal audits.
- One of the major challenges to integration seems to be the specific languages used by each world: Financial, Quality, Environmental, and so on.
- A balance remains to be found between all the different perspectives of the stakeholders of an organization. This is another debate for the future.

The title and sub-titles of the ASQ conference held in Philadelphia on September 17-18 said it all on the ongoing reflection about how organizations deal with the growing number of regulations and standards affecting them:

“How to Use ISO 9001 to Reduce the Risk from Sarbanes-Oxley”

“Beyond Compliance to Sarbanes-Oxley”

“Financial Benefits from Integrating your Management Systems”.

This conference was organized by Sandy Liebesman, who leads the SOX Q/E Team in support of the Sarbanes-Oxley Law, moderated by renowned quality specialists such as Paul Palmes, Donna Spencer, John Walz, and attended by many consultants and SOX, quality and environmental corporate experts.

At the time of the conference, September 2005, there is widespread awareness that striving to comply with each new set of regulations without relating each new compliance project with pre-existing programs is like reinventing the wheel and may prove very costly for subject organizations. The latest example of this well known silo effect is found in the way most organizations have implemented their SOX compliance project as a stand-alone and costly endeavor. The Sarbanes-Oxley Act is said to cost US listed companies over 5 billion dollars in 2005 in implementation of internal controls over financial reporting.

In the meantime a few advanced organizations, some of which were represented at the conference, dared tear down the walls of their internal silos and invite all experts to talk to each other, a first important step as Paul Palmes rightly pointed out. Financial to Quality to Environmental to Safety people talk to each other and compare their respective perspectives and languages, and eventually find themselves on the same boat and willing to support a more integrated view of their management systems.

Benefits of integration are pretty obvious and include, to name a few:

- Enabling top management and the Board of Directors to identify not only financial risks but all business risks, control them and prevent major surprises.
- Providing optimized results to all stakeholders
- Making corporate governance a pervasive cultural element throughout the organization
- Better use of resources
- Making all people throughout the organization aware of all stakeholders' perspectives and of the multiple facets of the performance of an organization, strategic, financial, quality, environmental, societal and so on.

The tools necessary to manage this integration are now largely developed. Ken Case, rightly we believe, reminded us that the Balanced Scorecard is currently the performance management system that is the best in sync with the integration of all management systems by tracking and aligning the multiple perspectives of an entity's performance.

As another example of how to look at integration, Harry Hertz and Kay Kendall, in two separate presentations, reiterated that integration is made easier through a system approach to Leadership, Governance, Ethics, and Organizational Sustainability as is the case in the Baldrige National Quality Program 2005 version. In particular Ethics is being given greater emphasis. Senior leaders are now seen as role models whose behavior is monitored by a governance body. Integration of all systems becomes a more naturally accepted approach because it really helps the organization in balancing value between all stakeholders in a longer term perspective.

Therefore concepts and tools regarding integration have been around for some time. So what makes it so difficult to implement and how to find synergies to make it easier?

Firstly as it was rightly pointed out, this increasingly complex regulatory environment is not a specific to the United States. SOX has cousins abroad, like the UK Turnbull Report, the EU directive on auditing, the Swiss code and many other countries' similar regulations. Globally, organizations are facing a increasing list of risks of non compliance.

Secondly, all agree that organizations are more prone to comply with regulations and standards when failure to do so entails heavy penalties. For example, as Mariann Zanardo and other environmental specialists pointed out, organizations know well how much it costs to deviate from FDA regulations. Now CEOs and CFOs face jail time if they do not comply with Sarbanes –Oxley, as Sandy Liebesman recalled. Therefore it is not surprising that after looking at a new regulation, organizations hurry up to meet deadlines in this new particular area and avoid penalties. Sitting back and thinking of better management practices comes later.

However, other factors are in play to push organizations toward a more integrated perspective of their management systems. For example, an indirect relationship between SOX and EMS already exists if we consider that environmental issues are already a target of SEC disclosure rules. As Bonni Kaufman (Holland + Knight) pointed out, SEC (Security and Exchange Commission) subject organizations must disclose material effects of compliance with environmental laws, including impact on earnings, competitive position and capital expenditures. Actually, the interest in environmental disclosures is growing- with issues such as global warming being now on the front burner.

So the question may be not whether or not SOX and the other multiple regulations/requirements (quality, safety, and environment) should be handled separately by an entity, the question is does basic good management practice require coherence, consistency, and alignment when issues are already intertwined? We believe the answer is yes. And to help in creating and maintaining this coherence, ISO standards contribute in offering their consensually adopted structures. Once again why reinvent the wheel? The organizations that do not adopt ISO or similar standards and tackle issues one after another as they come up run the risk of failing to address key issues or addressing them on a non timely and proactive basis. And as Barry Franklin, managing principal and actuary at Aon Risk Consultants recalls, directors are now more exposed to liability if they fail to address key issues.

Quality and Management specialists maintain that the management systems described by the international standards ISO 9001:2000, ISO 14001:2004, and other models of management such as the Malcolm Baldrige can support these tenuous compliance efforts, by providing a proven structure of controls and a continual improvement loop. In other words, why not use what already exists? Some observations made in organizations that strived to comply with SOX seem to support their claim. For example, a tremendous

amount of time and money was spent to assemble an internal control system, though the documentation for this was not put under control. Clause 4.2 of ISO 9001:2000 provides a long-established way of controlling a documentation system that SOX consultants and auditors could have adopted (or could adopt) to ensure that the costly internal control system they just set up is maintained in the future.

In fact there is a great deal of convergence amount among the various management models and frameworks we are talking about. For example, despite the fact that Sarbanes-Oxley focuses on internal controls over financial reporting, the COSO (Committee of Sponsoring Organizations) framework largely adopted by subject organizations has no such limits. Internal controls encompass actually three categories of objectives: financial reporting, operations, and compliance with regulations. The new COSO ERM (Enterprise Risk Management) framework published last year even includes a fourth category :strategic. Finally, it is striking that when compared all these management models, COSO, ISO, Baldrige, etc. follow a similar circular structure representative of the current consensus existing about how to run an organization efficiently.

Modern management entails a tone at the top, strategy and objective setting, risk assessment that these objectives may not be met, control activities to mitigate these risks, a solid information system to provide actors with the reliable information they need on a timely basis, a constant monitoring system to make the whole system remain effective and efficient, a feedback loop to make sure that the top management is thoroughly informed about the status and results of the system in order to act accordingly, and the whole thoroughly deployed at all levels of the organization. Therefore it makes a lot of sense to integrate the various management systems an organization uses since they follow the same structure and dynamic.

Even more striking is the fact that those management models reinforce each other. For example, the strong emphasis of ISO on controlling documentation or on continual improvement is a real plus brought to SOX, whereas the stringent penalties provided for by the Sarbanes-Oxley Act are reinforcing in subject organizations a culture of compliance that will make people feel an even more compelling need to meet all quality, environmental and safety requirements. This is why it can also be asserted that SOX supports ISO 9001:2000 and ISO 14001:2004! Good consultants know that well and advise their clients to adopt the optimized combination of all those models that fits the unique personality of their entity.

Another area where SOX may bring a significant contribution to existing management systems is the Information Technology (IT) control area that is hardly considered by ISO 9001:2000. Organizations subject to SOX have adopted CobiT (Control Objectives for information and related Technology) as a standard for good IT security and control practice. It makes a lot of sense to use CobiT (or a simplified version of it) beyond the SOX requirements to maintain a IT internal control system that covers all the applications of the organization. As a result, for example, data analysis which is an important element

of any management systems including QMS (clause 8.4) and EMS would benefit from higher data integrity and resulting decisions would be even better.

During this conference we were fortunate to hear from representatives of companies that have courageously embarked on the long way toward integration, trying to make the best of all the potential synergies described above. For example Lindy Olson, from Intrado, explained how they integrated the COSO framework and the Baldrige criteria, and how they integrated ISO and SOX audit programs.

When people collaborate, “talk to each other” as Paul Palmes likes to put it, this results in positive synergies. Paul Palmes and Donna Spencer told us how in some instances Sarbanes-Oxley non conformities were captured and managed utilizing the existing ISO non conformance system of the organization.

Based on the COSO framework, the internal financial audit should expand from its traditional scope more or less limited to financial matters to encompass the effective and efficient use of the entity’s resources. If the entity is to get the best use of its resources and create no overlap with other types of audits, it actually needs to combine financial audits with QMS and EMS audits. This is not that difficult if we consider that the audit methodology has been thoroughly revamped by use of the process approach and that ISO 19011 paved already the way to combined QMS and EMS audits, meaning that the essential work of identifying the common grounds to all audits has been done already. Adding the financial perspective is not difficult if a concerted effort is made to harmonize languages. Moreover it should be emphasized that quality and environmental auditors now have a certain experience of process auditing that they can share with their financial counterparts.

A hurdle to pass over may be who will lead the process of integrating internal audits. Our perception is that financial auditors who already have direct access to top management, audit committee, board of directors, external auditors, and are effectively supported by the Institute of Internal Auditors (IIA) consider that they should naturally lead this process. On the other hand, the American Society for Quality (ASQ) brings to the table a lot of experience in quality, environmental and process auditing but its audience rarely reaches the highest levels of the organization, even less the audit committee. Another area of potential friction between the two categories of auditors might be the role of the auditor as seen by the IIA that includes consulting services, whereas the quality world strives (?) to avoid conflicts of interest.

For us, one of the main obstacles to internal communication remains the language. Too few people can think of a link between ROE, ROIC, and lots of other financial acronyms and ISO, DOE, Cpk, SPC, and lots of other quality, environmental and safety terms.

One of the major challenges lying ahead may be how to reconcile the meanings that different people from different worlds put behind the concept of compliance, meanings that determine a specific culture. For example:

- Six Sigma people strive to reach no more than 3.4 defects per million of opportunities.
- Financial people look for “reasonable assurance”, define deficiencies (we simplify) as something that creates a more than a remote likelihood that a misstatement that is more than inconsequential will be detected. How many sigma is that?

A debate between those different approaches deserves to be initiated because integration does not mean confusion or merging of all concepts into mega concepts. Differences exist and will remain between the different perspectives of the various stakeholders of an organization. But to reach a balance between all those stakes, as the 2005 Baldrige invites us to do, a collaborative spirit is necessary so that the “point of balance” is well accepted by all.

There was not much time for debate during this otherwise rich conference. Let’s wait for the next one for this debate to happen.

October 10, 2005