

Using management systems for risk management and corporate governance

Nicki Dennis, BSI British Standards

Management systems have had a bad press; to some they cost too much, they stifle innovation and they are merely a guarantee of repeatability rather than quality. Despite these criticisms, there are also thousands of organizations that successfully use management systems to save them time and money, to improve their internal processes and procedures and to prove their competency to their customers. The reality for your organization is likely to be somewhere between these two extremes. This chapter will show you how using management systems alongside new risk management standards can help in two vital areas: risk management and corporate governance.

Corporate governance is the way in which corporations and other organizations are directed and controlled. The subject has been around for a while, ever since the problems arising from the separation of ownership and control of organizations has been recognized. Organizations such as Enron and WorldCom acted as catalysts

for corporate governance reforms; industry in both the UK and the United States has since become more focused on managing corporate governance appropriately and safeguarding stakeholders' interests. A spate of regulation has followed that has brought compliance issues to the very top of the corporate agenda.

A loud fanfare accompanied the introduction of the Higgs and Turnbull Reports in the UK, which aim to strengthen the role of risk management and clarify the relationship between auditors, boards and regulators. Within the United States, a juxtaposition of the Sarbanes–Oxley Act and the personal crusade led by Eliot Spitzer (Attorney General for the State of New York) to prosecute firms and individuals who break rules has led to one of the most significant changes in US Business Regulations in recent years.

Even with the introduction of new regulatory measures, it is clear that no firm is immune to the problems of poor risk management and corporate governance, and that initiatives introduced by the regulatory bodies such as the FSA should be viewed only as a base-line preventative measure.

With the stakes so high for both senior management and board members needing to take a grip on corporate governance, it should be in their best interests to implement additional initiatives that safeguard both their organization and their own futures.

Thus, it is recognized that there is a need for greater corporate responsibility and accountability than exists currently. This chapter aims to demonstrate the need for corporate governance and good risk management and includes a systems approach to adopting effective arrangements, in particular through the use of appropriate management systems.

Management systems

A management system is a way of running an organization that embraces its overall structure, its planning activities, responsibilities, practices, processes and resources for developing, implementing, achieving, reviewing and maintaining the policies of that organization. In short, it is everything about an organization. Thus when you are looking for a way of improving your risk management it makes sense to ensure that governance is at the heart of your chosen management system.

Central to all of this is the idea of 'risk'. An organization's top management should commit to establishing systems that will ensure that their strategic risks are identified and effectively managed. This system needs to operate at a strategic level and should encompass all of the organization's activities and the impacts they may or may not have on all stakeholders.

The obvious conclusion is that the most innovative organizations wishing to get ahead of the marketplace should embrace additional measures that safeguard their business and create a 'change-orientated' culture. Globally recognized 'Management Systems', such as ISO 9001 (for quality) and ISO 27000 (for IT security), can offer a unique combination of risk management and cultural change that encourages dynamic thinking and business improvement.

Within the context of corporate governance, the concept of using management systems as an effective risk management tool has been apparent for some time. Prominent examples include the *Turnbull Report*, which advocates the use of management systems as a mechanism to manage risk with regard to both the decision-making process and the day-to-day running of the organization. As it pointed out: ‘The system of internal control should be *embedded* in the operations of the company and form part of its culture.’

Risk as the ‘new’ quality

It is perhaps appropriate to draw parallels between the development of a quality culture in business throughout the 1980s and beyond with the current situation in risk management and corporate governance. This section describes how businesses have used standardization as the main process to drive through change and suggests how they might do so again.

Think back to how the so-called quality revolution happened. It was slow at first and then gained momentum as companies pushed ‘quality’ back through their supply chains. It became necessary to have a quality certification in order to even tender for some government projects – such was the confidence in the systems. Now we live in a very different world where our *expectations* are for products and services to ‘do exactly what they say on the tin’ as the advert says. The support structure for this *embedded* quality was impressive, accompanied by new job titles: quality managers, quality control analysts etc. A new language was built with its own jargon of Pareto analysis, root causes and TQM. A formal structure of institutes and societies were founded for continuing professional development – The Institute of Quality Assurance and the American Society for Quality amongst them. Quality arrived and dug in.

So how is ‘Risk’ similar to this? It is similar because I believe that in 20 years’ time our successors will look back aghast at the way we treated risk management at the start of the 21st century. In 20 years time risk management will be as embedded into our systems and processes as quality is today. The trick is to discover and describe how we get from where we are today to that position of truly embedded risk management. One way would be to copy the route taken by Quality. After all both quality and risk have their roots in statistical science. Quality developed from manufacturing as a part of the efficiency drive of the 1980s, when statistical process control charts helped operators to optimize control and improve on quality. Risk has its background in the mathematics of insurance risk. Both have strong links to probability, with the language of ‘expected outcomes’ and ‘Monte Carlo simulations’ being used at the academic end of both subjects. Quality has its own language and so does risk; the latter is one with which all will soon agree. The *ISO Guide 73* (new edition, due 2009) on risk management vocabulary is a good start in this tricky area. It defines risk as the ‘effect of uncertainty on objectives’ and risk management as ‘an organization’s culture, process and structures that are directed toward realizing potential gains whilst avoiding or limiting losses’. If all the various risk-related organizations around the globe could agree to use these two definitions, then that would certainly be a start towards a shared concept.

ISO 31000: an international risk management standard

For risk management the time is ripe for agreeing on the ‘shared concept’, and it needs to be a widespread agreement that includes governments, businesses, consultancies and trade associations. The International Standards Organization (ISO) is working on ISO 31000 which will be the first international example of this shared concept. The document is due to appear in early 2009, and I would urge interested readers to contact their national standards body (BSI in the UK, ANSI in the United States) and get involved in its consultation phases.

The British Standards Institute is also working in this area, but was not the first to become involved. Most readers will be aware of the Australian and New Zealand Risk Management Standard and also of the IRM/AIRMIC/ALARM Risk Management Standard (taken up and supported by FERMA, the European organization for insurance risk managers), although neither of these has yet caught the imagination of business in the same way as ISO 9000. None of these could be termed a complete Management System Standard in that they do not have any accreditation linked to them, but they will certainly support organizations that use them. Similarly if your organization does not use management systems the new standards will still be of use. BS 31100 will publish early in 2008 and will be the UK’s first attempt at combining good risk management guidance in the form of a standard.

ISO 31000 will be much broader based than anything that is currently available. It will, at least, include business ethics, corporate governance, reputational risk, IT risk, business continuity, operational risk and insurance risk as well as risk assessment techniques. Pulling all these themes together into a future formal management system standard may be unnecessary. Even as guidance, the rewards in terms of increased confidence both in and for business will be great. Other gains will surely be more stable insurance premiums, as after implementing the standards the better management of risks will lead to lower levels of risk transference to insurance providers. Certification schemes may help too (see later in the chapter). A good example is in the area of business continuity plans and the schemes that are available for BS 25999. A business will want to work with suppliers that have ‘good’ business continuity plans, but how should it define ‘good’, especially when it cannot get access to those plans as they contain competitively sensitive information. An independent accreditation to a formal standard is the perfect solution. Everybody can agree that they are all working to the same levels.

Implementing management systems

Management systems such as ISO 9001 require buy-in from senior management, but also require every employee to have an appropriate understanding of the policies and procedures relevant to them. Over time, this encourages a cultural change of open and honest communication that is led by example from the top. The process of embracing internal control in this manner not only provides an organization with an accurate

overview of the risks associated with its business operations, but will also help identify opportunities in areas such as reducing costs and increasing efficiency.

There are many different management systems available to help organizations manage operational risks. A combination can also be embraced to offer the organization a more holistic level of protection. The following is a selection of those management systems currently available:

- ISO 9001:2000 addresses the quality of products and services;
- ISO 14001 focuses on the environmental controls within an organization;
- OHSAS 18001 deals with health and safety within an organization;
- ISO 27000 deals with information security within the business;
- BS 25999 focuses on business continuity management and resilience.

All of these standards and specifications have one thing in common: risk management. They are also based on the ‘plan, do, check, act’ (‘PDCA’) model. The model is consistent throughout the new generation of management systems and allows for organizations to integrate more easily their management systems to achieve the holistic risk management model mentioned above. This is particularly relevant as many of the existing corporate governance solutions in the marketplace have a financial orientation.

In addition to easier integration with other management systems, the PDCA model encourages a culture of ‘continual improvement’ within an organization. This can help to improve efficiency and unleash the firm’s entrepreneurial spirit, whose potential was held back by the ‘tick box’ mentality created by the desire to comply with new legislative reforms.

Best practice

So what is it that organizations should be aiming for? What would constitute best of breed in this tricky area? In my opinion there should be a strategic policy at top management level to focus on managing risk for corporate governance. This should lead to specific policies and arrangements to deal with specific risks. In particular, the policy should encourage a positive culture within the organization to make certain that strategic risks are identified, removed, minimized, controlled or transferred. Specifically the policy should:

- reflect the nature and size of the organization and the strategic risks it faces;
- commit to ensuring that management competence is established to control risk;
- commit to ensuring that a culture is established to control or exploit the risk;
- commit to internal control audits to verify the systems and policy implementation;
- commit to regular review of the strategic risks;
- commit to reporting annually to shareholders, auditors and stakeholders as appropriate.

Certification

Third-party certification of a recognized management system can give internal confidence that appropriate measures have been implemented to prevent acts of poor corporate governance. Certification also gives external stakeholders (that is, regulatory bodies and potential investors) evidence of a sound management structure. This achievement could be the final requirement to attract investment or to satisfy the London Stock Exchange's criteria for a share listing.

Both the act of certification and the exit reports generated during the certification process can be used to produce an organization's corporate governance report. Furthermore, with revisions in company law and corporate manslaughter, certification to one or more of the management systems mentioned can be used by senior management in a legal scenario to show that appropriate policies were in place and adhered to.

Competitive advantage

A combination of legislative compliance and third-party certification to a formalized management system may be viewed as a burden, but it can also be a source of competitive advantage. First of all, compliance with legislation is not viewed typically as a unique selling point (USP). Addressing the law of the land should be taken as the norm and any organization that shouts from the rooftops that it complies with relevant legislation is not really going to have any credibility more than their competitors. While compliance with legislation should almost be taken as a norm, it is undoubtedly a good baseline from which to implement additional recognized methodologies. It is these additional risk management methodologies and solutions that will offer organizations a USP within the marketplace.

Implementation of one or more globally recognized management system demonstrates to all stakeholders that the management of risk is taken seriously, and gives confidence for both trading and investment purposes. Implementing and achieving certification to a globally recognized management system is an aspirational achievement: it is a way for a company to benchmark itself against its peers and know that it is doing well.

Potential investors can also take confidence from the fact that firms with certification to management systems such as ISO 9001:2000 will be focused on controlled growth and continuous improvement. Typically, financial investments are made on the basis of growth, and third-party certification can help give confidence to would be investors, both individuals and corporate. This is particularly important in this more cautious 21st century.

Furthermore, if the much-rumoured Corporate Governance Index is introduced, ISO registration would make a logical addition to the index's rating criteria. Trust is a significant business driver, and selecting those who manage risk appropriately is often difficult. A combination of a good corporate governance index rating and third-party certification can help demonstrate good governance and maintain trust.

The future

Following the actions of organizations that have caused a radical reform in legislation for corporate governance, firms have been forced to look closely at their risk management practices. While many of the reforms have been effective, it is clear that with scandals still hitting the headlines their introduction is not enough to protect stakeholder interests appropriately. With firms being expected to become great at ticking boxes to demonstrate compliance, perhaps the question should be asked whether this will leave enough resource for companies to be creative and drive themselves forward.

Management systems and, more specifically, a combination of management systems and the new standards to create an integrated system, offer a holistic level of risk management unsurpassed in the marketplace. While many board members within organizations that are not yet registered to a formal management system are debating how many boxes they have ticked, those that are registered are moving their organizations forward with the confidence that they have robust risk management in place.

With further reforms to corporate governance legislation inevitable, the only box that organizations will be required to tick in the future will be answered with a simple 'yes' or 'no'. The question will be: 'Do you have risk appropriately managed?'

References

M Robbins and D Smith (2000) *Managing Risk for Corporate Governance*, BSI, London