

Integrated Risk Management –

A holistic view of all risks to your business

CORPORATE GOVERNANCE

by Lindsay John Cox, Managing Director, Risk Governance Ltd

If you are the CEO of a major corporation today, there is massive pressure on you to demonstrate good governance practices, and provide tangible evidence that you and your board of directors are truly in touch with the workings of your business. These pressures are not only from the ever increasing number of regulations that demand this evidence, but also from shareholders, stakeholders and institutional investors, who need greater confidence in the management of the companies they invest in.

It is no longer acceptable simply to state what the threats to your business are, companies now have to quantify and prioritise them, and show detail and audited evidence of what mitigation activities are being employed to reduce the impact and/or probability of an incident occurring.

An analogy might be a mathematics exam, where it is not good enough to simply show the answer to a problem, but almost more important to show your 'working out'; how did you arrive at an answer? What was the logic behind the answer? Was there sound thinking behind the logic?

Everyone has a perspective on risk

Risk Management is performed by every employee in every business. Whether consciously or sub-consciously, everyone has a perspective on the risks associated with everything they do, and in some cases these are significant and in others they are insignificant. The objective is to make the important risks to a business visible by the business, and to be able to do so in a managed way, integrated with regular management reporting regimes. It is all too easy for important information and experiences to be lost with the passage of time, and by making the information visible, and recording it, a historical record can be kept such that previous decisions can be re-assessed with the benefit of seeing what was known then. This is extremely important to the audit function as well of course.

A new regulatory landscape

As we know, regulatory pressures have increased significantly for all companies, particularly those that are publicly listed. The latest wave of regulations have increased the focus on the operational side of business, covering accountability for financial reporting, internal processes, executive structure and management of risks, under the general heading of corporate governance.

With executives now accountable for the quality of risk assessment and control effectiveness in all aspects of their business, this presents a significant challenge for directors and officers. With so many regulatory requirements in every industry, it is practically impossible for an executive officer to realistically know what is happening everywhere within their company. But the regulations do not demand that they do know, simply that they can show that they have taken reasonable steps to make sure processes are in place to identify risks, implement, monitor and independently test controls, and that clear lines of responsibility and accountability for those risks and controls exists and can be proven.

This is where technology can play a vital role, in bringing together risk information from all parts of an organisation, such that a complete 'AWACS' view of the risk landscape for the business can be mapped. This provides tremendous value to the executive team as a 'dashboard' on the business.

This perspective is strongly endorsed in an article the *International Chamber of Commerce (ICC) UK Members Handbook*, by Walter Kielholz, Vice Chairman and former CEO of Swiss Re, and Prakash Shimpi President and CEO, Swiss Re Financial Services Corporation, where they state that "the risk map is the foundation of the holistic risk analysis project that is becoming an essential part of good financial management."

Figure 1. gives an example of how large amounts of differing risk information can be graphically illustrated using dynamic mapping techniques linked to the underlying data. Using this sort of capability gives management a broad perspective of all risks, whether regulatory, operational, market or Financial.

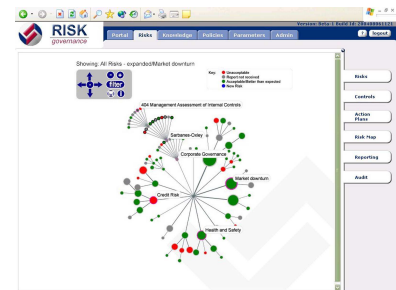


Fig. 1

To achieve this productively requires three key capabilities to be available in such a system:

1. A high degree of 'usability' to embed responsibility and accountability for risks deep into the employee hierarchy;
2. An open system architecture to facilitate the 2-way exchange of data from other systems;
3. Strong and dynamic electronic and physical reporting capabilities that allow manipulation of risk data for analysis, which can then drive value for the business.

Technology will support frameworks and processes

In the past, risk assessment has been an element of what the audit department might do on an annual basis, through workshops, site visits or reporting regimes that gather high-level information to satisfy crude reporting requirements to the board.

The requirement today and in the future is far more dynamic. Risk data must be identified, gathered, stored, aggregated, assessed and tracked for audit and comparative analysis, and to achieve that effectively it has to be stored in a database. That is a simple conclusion, but the real challenge is making sure the technology will drive participation by the risk community of risk owners and risk professionals alike. This means it must be both simple for use by the risk owner, to ensure valid acquisition of data on an iterative basis, as well as containing strong analytical capabilities for the risk and audit professionals such that real value can be derived from the information.

Getting people to participate

If we agree that to effectively identify and manage all the risks in a business, it demands widespread involvement of people across the business, which presents another significant challenge. To achieve this, there has to be a culture change, where every employee understands the importance of identifying and managing threats to their specific objectives, and the responsibility and accountability that they carry to do that diligently for the benefit of the company as a whole.

The only way to get participation from the masses is for them to see that it is a clear value to them as individuals and that it will improve their personal performance and strengthen the business as a whole.

Almost all of those that need to take responsibility for the identification and management of risks will **not** be risk experts, but regular business people within the company, where this risk assessment will be an additional task and responsibility for them. It is therefore even more important that their participation is seen to be little or no overhead on their regular activities, and that the information they provide is regarded as important.

Risk management is not an every-day activity for most

A 'risk owner', i.e. a person responsible and accountable for a risk or a number of risks, will probably be required to report on them according to some regular regime dependent on the importance and severity of the risk. Some risks may only need to be assessed and reported on annually, such as compliance to the rules related to 5-year auditor rotation under Sarbanes-Oxley 203 for example, whereas other more volatile risks may need weekly monitoring and reporting. Typically, most operational risks are likely to require status reporting on a quarterly basis.

Drawing the users into the application

The best way to gain participation by the risk owners is to draw them into the application through the one common environment to all; their electronic mail system; and by ensuring that risk is identified not as some adjunct activity but as an important component of managing towards their core goals and objectives. Providing reminders and alerts by email, that link directly into the risk-reporting environment through a link in the browser is how to achieve the first of these. This makes it easy to monitor and report on risk management activity, identify non-participants automatically, and provide an excellent management tool. Once a risk owner is in the risk-reporting environment, they must be able to complete their assessment and reporting activity simply and efficiently, with as much help and guidance available as possible.

Integrating information

As discussed earlier, risk information must come from all aspects of the business, and will be both qualitative and quantitative. High degrees of usability and collaborative technique to share knowledge and build collective wisdom

will help with the qualitative assessments, but quantitative information will also need to be integrated for aggregation and high level reporting.

Sophisticated risk assessment techniques have been in use for many years, and for many businesses they are fundamental to what they do. For example BPs oil and gas exploration and retrieval business is all about risk, and over time they have developed powerful systems to help understand and quantify their risks, which influence their strategic decisions. Banks and other financial institutions have also developed systems related to market and credit risk, which are core to their businesses. Power companies, pharmaceutical, automotive, in fact all industry sectors manage risks that relate directly to the products or services they provide, and historically these have been managed well.

The management of these risks may well be powered by technology, with complex algorithms applied to the data to arrive at a conclusion about risk exposure, and these are well tried, tested and trusted systems that will continue to provide that information. The challenge however is to get that information integrated into an enterprise-wide system for clear visibility of those in the context of all the risks to the business; strategic, operational, financial and regulatory. Thus, information must be gathered from all aspects of the business and the systems that support those, as illustrated in Figure 2.

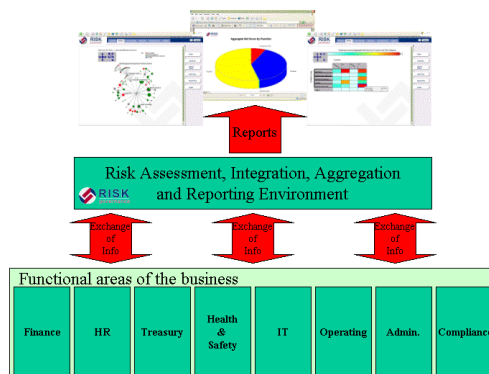


Fig. 2

The value in the data

An effective integrated risk management system will give tangible evidence that a company is embracing good business practice for governance, and will create a positive influence with city analysts. McKinsey research suggests that in the UK a company's evidence of strong governance practices can add up to 18% premium to a company's share price valuations, compared to a company that cannot show those practices.

Key values to an integrated and well managed risk and control system include:

- A lower regulatory capital requirement
- Lower operating costs and cost of finance
- Improved share price
- Improved quality and stability of earnings

- Lower insurance premium and/or reduced need to insure aspects of the business at all.
- "Prevention is better than cure" - Risks, properly identified and having clear parent/child relationships to other risks, will allow for early warnings of issues 'coming up the line' that ultimately could affect larger more important risks higher up the organisation. This will help prevent problems before they become materially threatening.
- Full audit trail analysis.
- If risks have controls in place to mitigate against them, and if those controls are managed and assessed and costed, then control-effectiveness calculations are possible, where an analysis of the cost of the control is measured against the resultant reduced risk.
- Actions can be 'kicked off' when risk thresholds are breached, risk appetites change, or changing conditions occur.
- Aggregation of risk information categorised in different ways can highlight areas of exposure not apparent when simply assessing individual risks to the business.
- Using raw risk data to populate sophisticated analytical tools for Monte Carlo simulation and the like. The quality of the analysis is only as good as the quality of the data, and by having an integrated, embedded risk management framework, valid data can be captured.
- Reduced losses (due to speed of response, actions & oversight, incentives, training, etc.)
- Improved prioritisation and targeting of resources (possibly through knowledge capture & leverage)
- Enhanced competitive position
- Improved probability of survival

Only by having this holistic view of the key areas of threats to strategic objectives can a CEO and his or her board of directors reasonably demonstrate that they are fully in touch with the workings of their business. Saying it is being done is one thing, demonstrating that it is being done is quite another.

Lindsay John Cox has some 18 years experience in the software industry. Lindsay is regularly asked to present at risk seminars, workshops and roundtable discussions at both private and public sector forums. He can be reached at:

*Risk Governance Ltd.
Surrey House
34 Eden Street
Kingston upon Thames
Surrey KT1 1ER
Tel: +44 (0)20 8481 3883
www.riskgovernance.com*

