International Conference on Risk Assessment and Management
Conférence internationale sur l'évaluation et la gestion du risque
Международная Конференция по Оценке и Управлению Рисками

24-25 November 2009
Geneva
Palais des Nations

A LESS RISK INTOLERANT SOCIETY: THE ROLE OF RISK MANAGEMENT PROFESSIONALS AND STANDARDS

Paul Taylor

Working Party on Regulatory Cooperation and Standardization Policies
ECONOMIC COMMISSION FOR EUROPE

Groupe de travail des politiques de coopération en matière de réglementation et de normalisation
COMMISSION ÉCONOMIQUE POUR L'EUROPE

Рабочая группа по политике в области стандартизации и сотрудничества по вопросам нормативного регулирования
ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ

UNECE, Geneva, Nov 2009

Paper from:

Paul Taylor, **Director of Ferma,**
Director of Risk Assurance at Morgan Crucible plc.

Introduction

WP.6 objective: To promote regulatory policies to protect the health & safety of consumers and workers, and preserve our natural environment, without creating unnecessary barriers to trade and investment.

The balance of regulation/control and the freedom to act or minimise barriers (as stated above) are critical to effective management of risk.

This paper presents the writer's and Ferma's ideas on:

1. The role of risk management professionals and standards in shaping society to be less risk intolerant and more responsible in managing risk
2. Guidance for business from the authorities. Learning from past experience
3. Co-operation between the business and the authorities in respect of risk management standards

Ferma, the Federation of European Risk Managers Associations represents approximately 5000 risk management professionals in 19 national risk management associations in 17 countries in Europe and Russia

The writer is a member of the Board of Ferma; Deputy Chairman of Airmic, (the UK Risk Management Association); has held corporate risk management positions in 3 UK FTSE 100 companies, a Swiss private company and is presently responsible for risk management and internal audit in Morgan Crucible plc in the UK.

1. The role of risk management professionals and standards in shaping society to be less risk intolerant and more responsible in managing risk

Today, society is becoming increasingly risk averse in many areas. This is partly due to the media, partly due to terrorism but also to developing "nanny" states where:

- When something goes wrong, authority's reaction is often to increase legislation/rules placing more restrictions on people and business rather than increasing education and understanding.
- The opportunity for taking risk is more limited (eg childrens' playground equipment being banned in schools, childrens' exposure to road risks increasingly experienced from the inside of a vehicle rather than as a cyclist or pedestrian). The emphasis is on **eliminating** risk rather than **managing it to an acceptable level**. By eliminating risk, the population will become more "risk ignorant", lose basic skills, have poorer health and may lose entrepreneurial skills.
- A "blame" culture is becoming more common (eg someone or somebody, and not the injured person, must be responsible if something goes wrong).The only winners in this situation are the legal profession.

Consequently, our world needs risk management frameworks and methodologies but also needs experience and education **to enable people to take risk but with a reasonable level of control** together with the acceptance that "zero" risk does not really exist.

Risk Management Professionals and the National representative associations can support governmental organisations and regulators in shaping a more risk tolerant society in a numbers of ways:

- Communicating clear messages that risk cannot always be eliminated but should be accepted as part of life.
- Working with the media to reduce the "sensational" aspects of the impact of risks and the demand for the blame to be allocated to someone else.
- Providing simple and effective methodologies to identify, assess and manage risks to an acceptable level. These can be included in communication to the public and to business.
- Education programmes to assist assessing and managing risks in everyday life. This includes domestic issues such as road safety, food safety, financial investments, etc.
- Providing experience in managing risk that helps people to understand and develop an appetite for and a tolerance to risk.
- Helping and advising authorities and regulators to ensure that any new regulation or litigation is measured and appropriate.

The key messages:

Risk cannot be eliminated or reduced to zero. Society needs to understand this and accept it.

Good Risk Management enables risks to be taken and managed to an acceptable level. Regulation and government communication should reflect this.

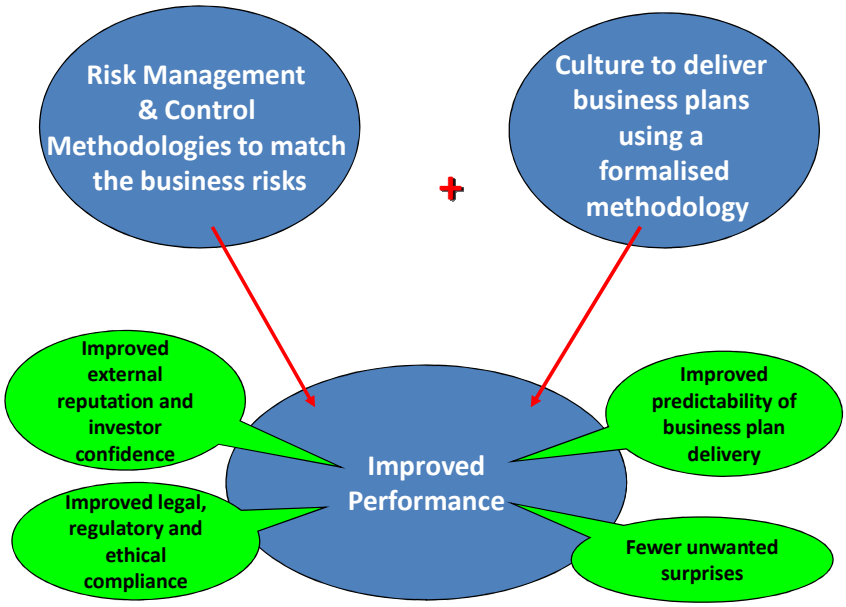
2. Guidance for business from the authorities. Learning from past experience

Increased regulation including corporate governance, has not prevented major failures of companies or banking melt-down. In some cases it has become a heavy and expensive bureaucratic process adding limited value and high cost to business. It has become a box ticking exercise.

In many European countries risk management requirements are already included in National Codes on Corporate Governance, as well as in the British Standard on Risk Management and the ISO Standard on Risk Management (due for publication before the end of 2009).

In addition to this, risk management professionals have published a number of guides on the subject including the UK Risk Management Standard published by Airmic, Alarm, IRM that has been adopted by Ferma and translated into a number of languages.

The more advanced organisations already implement Enterprise Risk Management. This is a framework to identify and manage all of the main business risks in a formalised and consistent way. This includes risks related to strategy, business planning, operational, supply chain, markets, political, social, economical, regulation, compliance and business ethics.



As shown above, the two key parts to delivering effective risk management are:

- Simple methodologies and tools that busy managers can use to enhance decision making and control. Ease of use and simplicity equates to increased likelihood that they will be used effectively.
- Creating and maintaining a culture to value and exploit the methodology

These two elements will deliver the benefits of improved performance that are illustrated above.

What guidance does business expect from the authorities?

- Risk management should be embedded in management processes in an organisation. As risk management processes and methodologies are still evolving, the current guidance is often at a “principles” level without much detail on implementation. Here is clearly an opportunity for risk management professionals to support authorities in providing more detailed guidance on implementation.
- The authorities should clarify and remind business of the consequences of poor management of risk particularly where this impacts third parties and stake holders in their organisations. Where fines/penalties do not act as a sufficient deterrent to inadequate risk management, then the authorities should review the need for change.
- At present much of the reporting required for business enterprises is standardised and presents minimal real value. Indeed in many cases, it could put a company at a competitive disadvantage to disclose publicly details of its key risks. Where reporting on risk is required, then the authorities should provide guidance or even clear direction on high quality and useful information.

What lessons have been learned?

A change in culture and behaviours is needed alongside appropriate regulation. This means using risk management tools and methodology as “part of the day job”. It includes monitoring, follow up and performance appraisal of their effective use. This requires training, education and demonstrating the benefits so that managers exploit those benefits and do not see the changes as purely bureaucratic. If the cultural change is not made, then the benefits of better management of risk will not be achieved and the processes will become compliance or box ticking.

Many well intentioned changes to regulation or standards have not necessarily achieved their original goal because they have not significantly changed behaviours. Typical examples are :

- Sarbanes-Oxley. The cost of compliance has been enormous but the benefits related to better management of the business have been more limited. Major company failures have continued in spite of regulation.
- ISO 9000. It is possible to be certified as having the quality processes in place, but have consistent **poor** quality.
- UK Turnbull code on risk management and control requires an annual assessment of business risks by the Board. In some companies this is a

compliance process that is separate from managing risk in the day to day running of the business.

In these cases, the compliance objectives were met, but the objectives of improving business performance were not necessarily achieved.

The Key messages:

The implementation of Risk Management standards and process are relatively easy – cultural and behavioural change is much harder. This is what makes the real difference

Too much regulation has a tendancy to produce "box-ticking" compliance and limited value reporting.

3. Co-operation between the business and the authorities in respect of risk management standards

Ferma and its member risk management associations have been actively involved in the preparation and review of many of the current risk management standards that have been published including:

- The Risk Management Standard published by Airmic/Alarm/IRM in the UK in 2002. This has been published subsequently by Ferma in a large number of languages.
- The British Standard issued in 2008
- The ISO Standard to be issued in 2009

There are other standards available including from the Australian Standards Organisation and the COSO guidelines from N America.

The UK and ISO risk management standards are intended to be non-certifiable standards at this stage and Ferma strongly supports this approach for several reasons:

- Formalised Risk Management methodology is still developing and is relatively new in many organisations when compared with other business processes such as quality management, health and safety, environmental management, etc.
- The choice of standards enables choice and further development. They are too immature to be certificated – This could perhaps be reconsidered in 5 years but the existing standards would require revision. Implementation guidelines would further assist implementation.
- The corporate governance frameworks are still developing in a number of countries with risk management being an evolving part of the framework.

Ferma seeks to work with other organisations to promote risk management knowledge. It already works with a number of European organisations to

promote and develop risk management. It would be happy to co-operate with UNECE on any projects to advance risk management including guidance on the implementation/application of standards.

The Key messages:

The current standards are good guidelines for describing risk management processes. Guidelines on their detailed implementation would assist users.

Ferma and its 5000 risk management professionals have the practical experience and knowledge to support UNECE on advancing practical risk management, standards and guidance.

A key part of improving management of risk is the recognition of professionals. There are a number of professional qualifications available for risk managers in Europe but none have the recognition or certification equivalent to accountants, lawyers, engineers, medical practioners, etc.

While the responsibility for managing risk is clearly with operational managers, risk managers are generally responsible for creating risk management strategy, framework, processes, leading initiatives, monitoring and control. These professionals have backgrounds and qualifications ranging from engineering, legal, insurance, finance and audit to health and safety, and corporate governance. The competences require to be responsible for risk management are being defined but are not yet globally accepted.

Internal audit is generally responsible for auditing and assuring the processes. There is some ambiguity related to the overlap of the audit role with risk management and the need for audit independence.

The Key message:

A qualification or certification for Risk Management professionals recognised by governments and professional organisations will help advance the evolution and acceptance of risk management.