RISK MANAGEMENT AND BUSINESS REGULATION

Bridget Hutter and Michael Power

The regulation of business and corporate risk management are inextricably related. Regulation is one way in which risks are managed in modern societies and corporate risk management is a form of self-regulation, although senior management would not articulate it in such terms. In practice, the distinction between regulation and risk management is becoming blurred as risk management blueprints influence the design of regulatory systems. This is particularly evident in the latest thinking of the UK Financial Services Authority, which is required to maintain market confidence and protect consumers. The FSA's new operating framework builds on its earlier risk based approaches to regulation and recognises that the nature and intensity of its relationship with a regulated firm will depend on the risk assessment of that firm. Accordingly, there is a pronounced convergence in form between the FSA's approach to regulation and the risk management practice of the very entities that it regulates. This trend is also visible in other areas.

Demands on governments to regulate risks are increasing. The by-products of new developments in such areas as food technology, public transport systems, e-commerce and lifetime financial planning may be unintended dangers to health, safety, and physical and financial security. Add to this concerns with the global impact of financial instability and environmental pollution, and it is clear that risk permeates regulatory agendas. Governments have typically intervened to regulate these risks, many of which are created by organisations rather than by nature, but they are hampered by two important factors. First, state regulation tends to be national, or at best regional, in scope, whereas risks are increasingly transnational in character. Second, the capacity of states to design and implement effective regulation of risks is constrained by the need to work with regulated entities.

Regulatory practice can take many forms. State regulation through the use of the law - popularly known as command-and-control regulation - is perhaps the best-known method. It is also the least loved by business and, according to regulation theorists, not always successful. But this is just one form of regulation and there are many others. For example, existing commercial incentives may be exploited or the state may co-opt the self-governing powers of the company. Systems of "enforced self-regulation" combine state and corporate regulation; they seek to penetrate the everyday life of the company and to harness its management tools in such a way as to align regulatory objectives and corporate strategy.

This style of regulation is now visible in many areas, such as environment, health and safety and corporate governance. For example, the Department of Trade and Industry played an important supporting role in the voluntary code of corporate governance in the UK (This was originally the "Cadbury" code introduced in the UK following the governance lessons learned from the collapse of the Maxwell business empire). The UK, like many advanced industrialised countries, relies upon a regime of standards requiring companies to develop their own risk management systems and internal rules. An important area where regulatory systems and risk management meet is the corporate internal control system.

Internal control

For many years, internal control was largely a private affair for organisations, at best only loosely connected to formal regulatory systems and a matter of interest to a few humble corporate

specialists, mainly auditors and quality control experts. However, this situation has changed dramatically. Systems of enforced self-regulation increasingly focus on the technical features of internal control systems, such as those for financial, environmental and occupational health and safety regulation in many jurisdictions. In the 1990s internal control also moved to the centre of discussions about corporate governance. In 1991 an influential conceptual framework for thinking about internal control (The "COSO" framework) was developed in North America by Coopers & Lybrand under the auspices of the Treadway Commission. COSO and other similar documents broadened the concept of control, making possible the alignment of corporate governance and risk management. In the UK this convergence of thinking about governance, risk management and regulation is epitomised by the recent "Turnbull Report".

The Turnbull Report and its underlying thinking supports a growing market for corporate advice in the public and private sectors, both in the UK and overseas. Its significance lies both in the specific recommendations it contains and also in the regulatory style that it signifies: the concept of control is broadened, tightly linked to risk analysis and enjoined as an imperative of "good" management. Disparate demands for risk management to become a senior executive preoccupation coalesce in Turnbull and in its support for a top-down, integrated corporate risk management policy. The ideal is that risk is analysed, controlled, communicated and monitored. In many respects these efforts to formalise principles of internal control simply repackage and extend an existing repertoire of control and risk management techniques. However, they also promote an ideal of integrated risk management.

Although risk and regulation are increasingly intertwined, they are not perfectly aligned, so compliance remains an important issue for organisations. Indeed, recent thinking suggests that the management of the risk of non-compliance is a key component of corporate risk management. Capital adequacy rules, health and safety regulation, and environmental protection regimes intentionally expose organisations to the risk of non-compliance risk precisely because regulation seeks to manage the risks faced by depositors, employees and local communities. In short, regulation is a form of risk management on behalf of individuals and forces organisations to address compliance risk. However, the very idea of compliance is far from being straightforward.

The management of compliance

It is not always clear what constitutes compliance. For example, regulatory laws are often vague, involving broad statutory standards and delegating a good deal of discretion to regulatory officials. Regulation is typically designed to be adaptable and flexible to changing technology, knowledge and the circumstances of individual companies and sites, so it necessarily leaves scope for interpretation. Thus, compliance is fundamentally a creative process involving negotiation and interaction between regulatory agencies and those they regulate.

Determining what is meant by compliance involves making an assessment of the risks associated with any given activity and their acceptability. One of the central difficulties of regulating industrial and commercial activity is finding a balance between the purpose of regulation - for instance, controlling risks to health and safety at work or reducing risks to the environment - and its cost. In practice, regulators refer to the absolute and relative monetary costs of regulatory demands and the general economic climate, both nationally and regionally, and between sectors and companies.

Consideration of these factors emphasises that regulation, not risk elimination, runs through the legal system, including the courts. For example, judgement was recently handed down in the UK

case of the oil tanker Sea Empress. In February 1996, an inexperienced port authority pilot ran the tanker aground at the entrance to Milford Haven estuary, spilling 72,000 tonnes of crude oil and causing widespread environmental damage to the Pembrokeshire coastline. The Milford Haven Port Authority was fined £4m costs, the judge noting that the level of the fine was based upon the authority's ability to pay and the gravity of the pollution. But the judge also added that he sympathised with arguments that the local area of Pembrokeshire could suffer "a double economic blow" with the incident and the level of the fine. In March 2000, the Court of Appeal reduced the fine to £750,000 on similar grounds.

Another key issue about the meaning of compliance is that our understanding of risk changes, as does public and managerial tolerance of risk. As the case of BSE shows, expert opinion may be divided over the sources and causes of risk and theories about both can change over time. Moreover political factors may intervene in determining acceptable levels of risk. The initial link between BSE and the brain disease CJD was made on the basis of ten Britons dying from a new strain of CJD. This led to a Europe-wide ban on imports of British beef and a vigorous campaign by the British Government to challenge the legality of the ban and the scientific evidence upon which the ban was based. Compliance is also determined by regulators' knowledge of organisations, that is, their specific knowledge about a site, its machinery, processes, equipment and personnel.

Based on experience and training, the regulator will make assessments of the organisation's compliance "culture" - its commitment to regulatory objectives, its record of compliance, the quality of its management and its capacity to comply. These considerations influence the regulator's motives to intervene in a company's affairs and are often formalised as guidance for regulatory officials. For example, the UK Environment Agency's criteria for prosecution include the extent to which non-compliance could have been foreseen, the intent of the offender, the history of offending and the offender's attitude. The application of these criteria will of course depend on the willingness and ability of an organisation to self-regulate.

So, what does this mean for "compliance risk management"? If compliance is emergent, the outcome of negotiation and interaction, businesses may be genuinely unsure what compliance is. Furthermore, companies and the managers within them may differ greatly in their understanding of regulation. Research shows that while small businesses are often confused about regulation, large companies use regulators as a resource and source of information. Small companies tend to be less able to self-regulate and more ready to accept regulatory requirements, whereas large companies are more inclined to challenge regulation. Attempts to co-opt corporate risk management systems or to guide and advise them are not well understood by business, who tend to perceive regulators in a policing role.

Studies of corporate responses to occupational health and safety regulation suggest that there may be wide variations in the attitudes and expectations of safety departments in large companies. The reason is that guidance about compliance with occupational health and safety regulation is differentially interpreted across a large organisation. A case study of the UK's former nationalised rail company British Railways, found that departments implement the general health and safety commitment in their own way. Consequently, there was no standard response across the organisation. Poor communication emerged as a main obstacle to successful compliance risk management. Fragmentation of the company meant that important risk information was kept at a departmental level. More generally, when risk information is kept isolated in separate divisions or departments of an organisation, understanding and decision-making at the senior level becomes impossible. This is a well-documented feature of "man-made disasters".

The implications

These examples suggest that compliance is a complex phenomenon at the interface between risk and regulation. Regulation is both a form of risk management and a source of compliance risk. As regulation seeks to operate increasingly with the grain of organisational life, risk management in its broadest sense represents the continuation of regulatory programmes within businesses. Accordingly, the inside of the organisation is increasingly recognised as a "regulatory space" in which the various facets of compliance are determined.

The process of convergence between regulatory ambitions and organisational priorities is not smooth or guaranteed. Corporate responses to regulation are poorly understood and little is known about the extent and normality of compliance. The regulatory process involves multiple agents: inspectors are co-opted into organisational processes at the same time as aspects of risk management are outsourced. Compliance officers and corporate risk managers wrestle with their dual roles as regulator and as internal advisor. Auditors and consultants also play an increasingly influential role in determining the understanding and management of compliance.

In short, the corporation is becoming an arena for intense competition as internal and external auditors, legal specialists, heath and safety officers, inspectors and others seek a pre-eminent foothold in the market for internal advice, and in the market for defining regulatory compliance. Accordingly, the policy agenda for the future is use these resources to improve the alignment of corporate risk management practices and regulatory regimes. Yet since the active market for interpretations of compliance is global, the capabilities and horizons of national regulators are likely to remain challenged in the future.

This article first appeared in the Financial Times Mastering Risk series

www.ftmastering.com

Further reading

London Financial Services Authority (2000) A New Regulator for the New Millennium, chapter 2.

Ayres, I. and Braithwaite, J. (1992) Responsive Regulation: Transcending the Deregulation Debate, Oxford: Oxford University Press.

The Committee of Sponsoring Organisations (1992) Internal Control - Integrated Framework

"Internal Control: Guidance for the Directors of Listed Companies Incorporated In the United Kingdom" (1999) London: Institute of Chartered Accountants in England and Wales.

Power, M. (2000) "The New Risk Management", in European Business Forum 1 (1): 60-61.

Hutter, B.M. (1997) Compliance: Regulation and Environment, Oxford: Clarendon Press.

Hutter, B.M. Regulation and Risk, Oxford University Press, forthcoming.

Published by the Centre for Analysis of Risk and Regulation at the
London School of Economics and Political Science
Houghton Street
London WC2A 2AE

(This article was first published in the Financial Times Mastering Risk Series, 2000)

ISBN 0 7530 1429 7

Printed at the London School of Economics and Political Science, October 2000