Theme Paper

Global Convention on Corporate Ethics and Risk Management

Corporate Ethics and Risk Management in an Uncertain world

17-18th February, 2017

Bombay Stock Exchange, Dalal Street, Mumbai, India

Prof. Colin Coulson-Thomas*

Ethics and risk management are interrelated. They represent the essence of responsible and sustainable business which is based upon trust, the building of mutually beneficial relationships with shareholders, an understanding of risk and the balancing of risk and return.

Directors and boards need to ensure that policies, frameworks and governance arrangements are in place to ensure ethical conduct and decision making and effective risk management. They must also ensure their own conduct and the vision, mission, values, goals, objectives and priorities they set are conducive of them and do not undermine them.

Unethical conduct can damage relationships and significantly increase a range of risks, whether the incidence of fraud or damage to a corporate reputation. It can therefore have both short-term and long-term consequences. In some circumstances these can prove fatal for a company's future prospects and threaten its survival. Similarly, the failure to address certain risks can also prove catastrophic. Yet the taking of reasonable and calculated risks is at the heart of entrepreneurship. The courage to venture and explore is necessary for innovation and if progress is to occur.

Directors themselves need the courage to challenge when and where it is appropriate and/or they have concerns. To do this effectively they need to understand what questions to ask in relation to ethics and risk management. This theme paper sets out some areas for questioning and discussion at the 2017 Global Convention on Ethics and Risk Management.

Ethics, Corporate Conduct and Business Decision Making

Ethical and balanced decision business making can establish confidence, engender trust and build a reputation for honest dealing. In the case of decisions that come to the board, directors should aim to set a good example and be individually and collectively accountable for their own conduct. In some circumstances they may become personally liable for their actions.

As well as being directly impacted by board decisions, the behaviour of others may be influenced by the tone set from the top. While directors may have their own sense of what is ethical, fair or reasonable in particular circumstances, stakeholders and other parties may form their own and different judgements. These may reflect individual, group or local opinions, views and values.

External views of what is acceptable, and indeed legal, may vary from place to place and from time to time. Directors will be expected by regulatory and legal authorities, ethical investors and other stakeholders to establish, monitor, observe and enforce certain norms. At the same time, they also need to be sensitive to changing ethical requirements and perspectives, and aware of the possible implications of certain actions. What should a company's values and ethical norms be? How should they be expressed and communicated? Should a company have an ethical position on certain issues?

How can a board create a ethical climate within which governance and management activities can occur? How might they ensure it is appropriate for the nature of a company's operations, the applicable legal and regulatory framework, stakeholder requirements and expectations, a prevailing moral climate and the challenges and opportunities that it faces?

In relation to ethics and corporate conduct, should a board be a follower of trends and just do what is legal and allowed, or should it give a lead and endeavour to raise ethical standards? How should it articulate and account for corporate social and ethical values? Are ethical standards, a code of practice and ethical guidelines required? If so what areas and issues should be covered and in how much detail? Will an ethical helpline and support tools be required?

How might a board best ensure ethical and legal compliance? Is an ethical and legal compliance management system required? If so, who should be responsible for this? How should such a system or framework be linked with a company's risk management approaches, system and processes, so that integrity and other corporate values, ethical principles and a corporate culture can best contribute to the management of risk?

Risk Prevention, Mitigation and Management

A degree of risk is inevitable in business operations and to obtain higher returns, innovate and secure market leadership one may need to adopt a higher risk strategy. What are the risks of not innovating and not being prepared to take risks? A board should establish its risk appetite. It should agree the level of risk it is prepared to accept in respect of different areas of corporate operation and a strategy and policies for the management of risks.

Decisions about whether or not and how best to transfer risk also have to be taken, such as whether of not to hedge or insure against certain risks, depending upon the costs and practicalities involved. Processes and practices need to be put in place for the identification and management of risks. How complex and comprehensive do these need to be once the most likely and significant risks have been addressed?

Who is or should be responsible for risk management? Paradoxically, establishing clear responsibilities for risk prevention, mitigation and management and allocating them to particular individuals can sometimes increase risk if others then assume that risks are “taken care of” and they are not themselves alert to risks. A healthier approach may be to additionally make sure that all staff reflect upon and address the risks inherent in their roles and corporate operations they are involved in. They should be encouraged to report any risk concerns they might have.

Directors need to make sure that executives are not so focussed upon listing and addressing individual risks that they overlook the interrelationship of different factors. A development in one area can often have consequences elsewhere. For example, too many errors and exceptions can lead to overload and bring down a system.

Assumptions and business models should be periodically challenged. A rigorous assessment of the implications, consequences and dependencies of certain corporate strategies, policies and projects might reveal exposure and vulnerability. Just in time approaches might result in shortages in a variety of areas if there were an interruption to certain supplies. Systems and processes need to be resilient and able to withstand the simultaneous materialisation of multiple risks.

The Board and Risk Management and Governance

There are many other areas in which directors could ask questions. Processes and systems need to be adaptive as well as resilient, as the nature and source of risks can change. As old ones are addressed so new ones can emerge. Are risk registers and management reports relating to risk over generalised? How realistic are they in relation to assessments of risk and planned corporate responses? Do they provide sufficient evidence and explanation to inform the board's own reporting of risk to shareholders?

Are people within the organisation and its supply chain aware of the diversity, incidence and severity of some categories of risk? For example, while overall relationships with customers might seem acceptable, are there particular relationships with key customers that are especially at risk? A small account could have growth potential and might become strategically significant in the future.

How well positioned is a company in respect of certain categories of risk? Is the risk culture of the organisation appropriate in relation to the company's activities and operations and the opportunities it faces? Is it too week or too strong? A degree of balance is required. An excessively risk averse culture could lead to stagnation, but a step change increase in risk might be unsettling for some investors. High risks in certain areas might be tolerable when they are balanced within a portfolio of activities, operations and products by other items with lower risk profiles.

How should the board establish and communicate its risk appetite and tolerance? Which stakeholders should be involved and how should they be engaged? Does the risk culture of the board match that of the organisation and its aspirations? If not, what changes are required and how might they be brought about?

What are the risk oversight functions of the board and how effectively are they being discharged? For example, is annual reporting of risk to shareholders fair and balanced? Would confidence accounting present a clearer picture? Within the governance structure, what arrangements have been made for risk governance?

What external and objective advice does the board receive in relation to risk? Does the audit committee ensure that the work of internal and external auditors is risk based? Should there be separate risk and internal audit committees? Is there an agreed internal audit charter that sets out the rights and establishes the independence of the internal auditor and his or her team? Overall, from a board perspective, what more needs to be done to build a risk resilient enterprise?

Risk Management Frameworks, Approaches and Responsibilities

Has the management team established an effective risk prevention, management and control framework? Are people equipped with the skills, tools, techniques and other support they need to effectively operate it? Are the techniques used adequate in the situation and circumstances?

Does the company's risk management framework, policies and practices extend to the supply chain? In particular, are supplier risks and the risks of activities such as outsourcing and joint ventures assessed and managed, including by collaborative action where relevant.

Is the risk register a living document? Are the prioritisation of risks, mitigation measures, responsibilities and residual risks regularly reviewed? Are risk reports colour coded to reflect likelihood of occurrence and impact? Is the direction of travel given? Are movements in relation to high priority “red rated” risks monitored by the board? Are there trigger points at which additional advice is sought and/or further resources deployed or other action taken?

Are risk factors understood, appropriately categorised and mapped? Are the risk assessment criteria

used reasonable and fair in the circumstances? Do the results of risk analysis inform business and management decisions? Are they inhibiting or supporting innovation and entrepreneurship?

How outward looking and inclusive does risk management need to be? Are the risks of major and strategic customers and business partners understood? Are business opportunities being identified for how the company might use its capabilities to help customers and others to mitigate, prevent or manage the risks they face?

How are activities relating to risk managed? Is there a Chief Risk Officer (CRO)? If so, how is the role of the CRO changing? What skills and experience are required by risk management professionals? What steps are taken to ensure that others do not abdicate their responsibilities in relation to risk by leaving too much to the CRO and his or her team?

What should be done to ensure that any approaches to risk management adopted are current and that knowledge of changing risks and how they might best be addressed are up-to-date? Within the governance structure, how does the CRO relate to and collaborate with the audit, compliance, finance and legal teams? Are regular formal and/or informal meetings held to identify and discuss patterns, trends and common root causes?

Corporate Action to Combat Fraud

Where people are involved the risk of error and fraud is ever present. The performance of most people is variable and their susceptibility to mistakes and temptation can also change with personal circumstances. A corporate team is only as strong as its weakest link. One slip or click could open the door to a fraudster or hacker.

The very thought of surveillance and the monitoring of staff can sometimes undermine trust and trigger negative reactions. However, managers and HR personnel need to be vigilant. They should be alert to changes of behaviour and circumstances that might suggest someone is under pressure and/or up to no good. Is working late and a reluctance to take holidays evidence of commitment, or an indication of the possible perpetration and concealment of a fraud?

Are people throughout the organisation alert and aware of the many areas and situations in which fraud can occur? Is their vigilance periodically tested, for example to find out how many of them will click upon a suspect looking email created by the company and leading to a warning page? Are they regularly issued with anti-fraud advice?

Are all members of staff expected to observe certain basic principles of conduct, such as avoiding obligations to others, declaring interests and avoiding conflicts of interest? Where contraventions occur, are appropriate steps taken? Is this communicated to others as a warning and a guide? In some organisations there is a tendency to hide instances of fraud. Is the board sighted when frauds occur? Are incidents disclosed, properly reported and adequate follow-up action taken?

Does the board question the adequacy of internal control arrangements? Are purchases split to avoid internal control limits? How likely is it that internal and external audit checks will uncover hidden bribes and “on the side” commissions? Would they catch the processing of fake invoices, the misuse of company facilities and resources, or the favouring of a particular supplier? What proactive monitoring and preventative measures are taken to protect the company against organised and/or systemic corruption, bribery and fraud in particular places and markets?

Unpredictable Risks and Natural Disasters

Some boards regularly review schedules of risks notified by management, but rarely consider less predictable and external risks such as natural disasters, an act of terrorism or political instability. Do the results of issue monitoring and management exercises, that involve identifying and ranking developments in the external business environment and assessing their impacts upon a company and its customers and supply chain feed into the risk management process? Is the risk management team involved in deciding what action a company needs to take in response, whether to address a challenge or seek to exploit and opportunity?

Certain unpredictable events could potentially have huge implications for companies and their operations. Corporations have had their assets and operations nationalised as a result of regime change. How resistant would offices and plants be to high winds or a tsunami or earthquake? How should a company cope with a terrorist attack, a pandemic, a sudden interruption to its supply chain, the loss of key staff, or a break down of law and order? Are contingency arrangements and back up and recovery plans in place? How resilient are a company's finances and business model?

Companies that operate internationally can sometimes find that the risk profiles of their different local involvements will vary significantly. Such involvements might expose them to geopolitical, economic, trade and other risks. These could range from a repudiation of debts to the sudden devaluation of currencies.

Some risks are or might be insurable at a cost, while others may need to be borne. How does a company assess unpredictable and/or uninsurable risks? Are these spread across a range of activities, or is there disproportionate exposure in particular markets? Are such risks and a distinctive risk management perspective taken into account in related and strategic decision making? For example, a strategy of focusing upon a core business has resulted in many companies being less diversified and having “more of their eggs in a single basket”.

Systemic Risks and Shocks

The continuing operation of many businesses as going concerns is dependent upon the effective operation of the banking and financial system and the activities of governments, regulators and the legal system in the major markets within which they operate. Even in advanced countries, one cannot assume a banking and financial system will remain free of the challenges and loss of confidence that occurred in the period 2008-9 and which led to bank failures and bailouts.

Governments and regulators take various actions to support banking systems and sectors such as the utilities upon which most companies and citizens depend. These can range from changing licensing conditions and reserve requirements, through inspections and periodic stress testing, to interventions such as quantitative easing when the going gets tough.

The consequences of banking failures and interruption to the regular operation of the financial system could have catastrophic consequences for highly leveraged companies and businesses that have cash flow problems. Should businesses other than banks also regularly review their reserve and liquidity requirements? Should they arrange independent stress testing of different aspects of their core operations? Could bartering and/or the sharing economy provide new or fall back options?

Boards should be aware of important dependencies. For example, do they know for how many days they could operate in the absence of banking support and/or the ability to carry out financial transactions? What contingency arrangements are in place with customers, creditors and suppliers? Should a company know which external entities would be supportive and which of them, whether by choice or because of the situation they are in, would be forced to “pull the plug”?

Major companies may be in a position to collaborate with government and other external parties to help ensure the resilience of the banking and financial system. Should they participate in contingency planning for back up and other arrangements for enabling essential services to continue? What steps could be taken to protect the interests of customers, staff and other stakeholders in the event of a financial crisis or utility failure?

How resilient are collateral, monitoring and regulatory arrangements in corporate and retail banking? Will the Basel capital regulatory framework and other arrangements, requirements and standards be able to cope? What would happen if banks again lost confidence in each other? How might a company be impacted by decisions of other parties within the financial system? For example, what would happen if loans were called in earlier than expected or debtors defaulted?

Managing Risks in the Financial Sector

Systemic risks relating to the banking and financial sector are of particular concern to directors of financial institutions. Like directors of utilities they are responsible for entities upon which other organisations and many people are dependent, and for whom alternative arrangements could involve much inconvenience and significant costs.

Have the lessons of the failures and bailouts that occurred in the period 2008-9 been understood? What minimum standards should be required of financial and lending institutions, and at what point should public and regulatory intervention occur? Are satisfactory and resilient mutual support and other arrangements in place if a loss of confidence results in panic withdrawals or asset sales?

Within financial services, the business of insurance companies is risk and reinsurance. Expertise may be required in a wide range of risks. In such specialist areas, directors should consider whether boards contain sufficient sectoral understanding to discharge their responsibilities.

Are changes in economic factors such as inflation, interest and currency rates, market conditions and government policies being monitored? Are contingency arrangements in place to deal with the consequences of sudden and significant changes? Where others might jump ship, what steps are being taken to avoid being left with the highest risks, worst prospects and biggest potential losses?

As already mentioned, risk and return are often related. Could the wider adoption of performance support tools enable more companies to end the traditional trade off between risk and return and simultaneously increase returns and prevent and/or contain risks?

Certain activities such as innovation, new product development, entering markets, funding new ventures or changing a business model can incur relatively high risks. However, they may be undertaken in order to secure increased and more sustainable returns. Within a diversified portfolio of ventures and initiatives, one hopes that the returns from those that succeed will more than cover the costs of those that fail.

Sources of fresh capital for expansion and the support of new ventures are changing. In some jurisdictions, less emphasis is being placed upon stock exchanges. Many smaller enterprises in particular are making greater use of organised crowd funding. Are adequate steps being taken to spread risks and fairly share the costs of failures?

Cyber Security and Risks

Various risks are associated with greater connectivity. A company's defences are only as strong as

the weakest link across the various networks to which its people and operations are connected. The route in to a network could be a fridge in a kitchen connected to the internet, or the one employee who clicks upon an attachment without questioning the covering email. The internet of things is a frontier of opportunity for hackers. For many companies the issue is not whether a breach will occur, but how to limit the damage and recover quickly when it does.

In relation to cyber security and fraud, are emerging and mutating threats being monitored? Is information about identified threats, breaches and responses being shared with other organisations? Are cyber security and information governance policies being regularly reviewed? Are contingency arrangements, threat scenarios and planned responses periodically tested?

What checks are made or should be made to avoid money laundering? What steps are being taken to avoid the loss of strategically significant intellectual property and unapproved access to personal information when data thefts occur? At what point and by what means will those at risk as a result of a corporate data breach be informed? How will those who suffer loss be compensated?

A key question is the speed with which defensive and anti-malware software, and data and system security, can be updated quickly as and when the need arises. Can this be done at weekends and over public holidays if new threats emerge? Are strategies and measures in place to channel and contain hackers and, where possible, to retaliate and/or increase their costs?

Do adequate security measures extend to a company's supply chain, corporate data that is held externally and corporate systems that are operated by third parties? How secure are “working from home” equipment, customer support facilities and portable devices? What advice and support is given to staff and business partners in these areas?

International Collaboration and Standards

What role can and should international frameworks and standards play in enterprise risk management (ERM), internal control and fraud deterrence and the prevention, mitigation and management of risk? Are they helpful in encouraging structured and systematic approaches, or do they operate like an anaesthetic and put people to sleep? Do they encourage them to tick compliance boxes and then relax? Is conformance reassuring or could it reduce vigilance?

There is much that companies can do to address their particular issues, situations and circumstances. In addition, they can also learn from the experience of others and contribute to collective efforts and international developments. Are boards doing enough to support international collaboration? Should more companies comment on the ERM framework and guidance issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and/or the ISO 31000 risk management standard published by the International Organization for Standardization (ISO)?

What are the advantages and disadvantages of COSO and other frameworks and standards such as ISO 31000? How applicable are they to different forms of company? How might they best be used? Should they complement and supplement corporate processes and practices and current risk based approaches to risk management and internal and external audit? What changes are required? Is more or less detail and better guidance needed?

What developments in international collaboration law, regulation and oversight would increase cyber and international network security? How can companies best contribute to these? What action can and should governments, international organisations and companies take against sources of cyber espionage and state sponsored hacking? Where are there gaps in defences and inadequate counter measures? What are they and how might they best be plugged?

For various reasons companies are often unwilling to disclose certain breaches of security, even to law enforcement agencies. This reluctance and lack of openness limits the extent to which others can learn from their incidents, investigations and findings. Should companies do more to share their experience and resulting lessons with peer organisations and national and international authorities?

Striking the Right Balance in Action and Reaction

In relation to ethics and risk, contemporary companies operate in an uncertain world. Boards face multiple challenges and confront sensitive issues. Circumstances require them to take difficult decisions in terms of preventive measures and how to respond to certain events. Discussion with ones peers can help directors to get an overview of the ethical and risk landscape. It can highlight the interaction of different factors and help to clarify what is important and needs to be addressed.

Preventive measures, incidents and responses can have both immediate consequences and wider implications. Listening to ones peers and learning from them can be helpful for building resilience and a balanced perspective. When responding to incidents one may need to both recover and move forward. A case study might reveal how this was done, or a balance struck between specialist input and complex arrangements where these are required and general awareness and vigilance across an organisation. For a multi-layered defence both are likely to be required.

When unwelcome risks materialise, frauds and other incidents occur and/or disasters strike, an organisation that is prepared, insured, able to respond quickly and is both ethical and practical may be well placed to cope. Panic, self serving responses and over reactions can compound any damage caused. Those seeking a strategic supplier or an investment to hold are likely to favour level heads and resilience in adversity. Having a moral compass and reacting in a proportionate, fair and responsible way can help a company and its board to restore confidence, maintain trust and build relationships with stakeholders.

*Author

Prof. Colin Coulson-Thomas advises boards and has helped directors in over 40 countries to improve director, board and corporate performance. He leads the International Governance Initiative of the Order of St Lazarus, is Chancellor of the School for the Creative Arts, Director-General, IOD India, UK and Europe operations, and chair of the Audit and Risk Committee of United Learning. Author of over 60 books and reports he has held public appointments at local, regional and national level and professorial appointments in Europe, North and South America, Africa, the Middle East, India and China. Colin was educated at the London School of Economics, London Business School, UNISA and the Universities of Aston, Chicago and Southern California. He is a fellow of seven chartered bodies and obtained first place prizes in the final exams of three professions.