Risk Governance and the Board

*Prof. Colin Coulson-Thomas

*Prof. Colin Coulson-Thomas is IOD India's Director-General, for UK and Europe Operations, also holds a portfolio of board academic and international roles, and has advised directors and boards in over 40 countries.

IOD India's 2017 Global Convention on Corporate Ethics and Risk Management will consider a number of interrelated areas that should be of concern to directors. Ethics and risk management represent the essence of responsible and sustainable business which is based upon trust, the building of mutually beneficial relationships with customers and other stakeholders, 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 governance and management. They must also make sure that their own conduct and the vision, mission, values, goals, objectives and priorities they set are conducive of them and do not undermine them.

The failure to address certain risks can 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. Hence, in relation to risk governance, directors need to achieve a balance between contending factors and there may be difficult choices to be made. This article will consider some issues directors may have to consider and questions they should ask.

The Board and Risk Management and Governance

A degree of risk is inevitable in business operations. To obtain higher returns, innovate and secure market leadership one may need to adopt a higher risk strategy. Not innovating and being risk averse can condemn an enterprise to stagnation. A board should establish and communicate its risk appetite and agree the level of risk it is prepared to accept in different areas of corporate operation. 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 which involves setting a strategy and policies for the management of risks and monitoring the performance of those to whom risk and security responsibilities are delegated?

Policies could cover the transfer of risk, such as whether of not to hedge or insure against certain risks, depending upon the costs and practicalities involved. They could establish criteria and thresholds for reporting and guiding management responses. Directors need to ensure effective processes and practices are 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?

Assumptions and business models should be periodically challenged. An assessment of the implications, consequences and dependencies of certain corporate strategies, policies and projects might reveal exposure and vulnerability. For example, should an interruption in certain supplies occur, might just in time approaches result in shortages? Corporate systems and processes need to be sufficiently resilient to be able to withstand the simultaneous materialisation of multiple risks.

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?

Corporate Risk Management

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? When addressing questions read the road ahead. A small account might have growth potential and could become strategically significant in the future.

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

How well positioned is a company in respect of certain risks? Is the risk culture of the organisation appropriate in relation to its activities, its operations and the opportunities it faces? A degree of balance is required. An excessively risk averse culture could prevent progress, but a step change increase in risk might be unsettling for some investors. High risks in certain areas can sometimes be balanced within a portfolio of activities and products by other items with lower risk profiles.

Processes and systems need to be adaptive as well as resilient. The nature and source of risks can change. As old ones are addressed so new ones may 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?

Risk Management Frameworks, Approaches and Techniques

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? 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? Does the company's risk management framework, policies and practices extend to its supply chain? In particular, are supplier risks and the risks of activities such as outsourcing and joint ventures assessed and managed? Does this involve 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?

Risk Management Responsibilities

To whom should risk management responsibilities be delegated? 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 other people do not abdicate their responsibilities in relation to risk by leaving too much to the CRO and his or her team?

Responsibilities for risk prevention, mitigation and management need to be delegated with care. Allocating them to particular individuals can sometimes lead to others assuming that risks are "taken care of" and not themselves being alert to risks. A healthier approach may be to both delegate and ensure all staff reflect upon and help to address risks inherent in their roles and any corporate operations they are involved in. Any risk concerns they might have should be reported.

What should be done to ensure that adopted approaches to risk management are current and that knowledge of changing risks and how they might best be addressed is 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?

Anti-fraud Policies and Practices

Where people are involved the risk of error and/or 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 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 a company 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 organisation 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? Are these 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 and properly reported? Is adequate follow-up action taken?

Does the board question the adequacy of internal control arrangements? Do people split purchases 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. Does issue monitoring and management involve identifying and ranking developments in the external business environment and assessing their impacts upon a company and its customers and supply chain? Do the results feed into risk management processes? Is the risk management team involved in deciding what action a company needs to take in response?

Certain unpredictable events might potentially have huge implications for companies and their activities. Corporations have had their assets and operations nationalised as a result of regime change. How resistant would offices and plants be to gales, floods 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 sometimes find that the risk profiles of their local activities vary significantly. Particular 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 certain 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 utilities, 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 with vulnerable cash flows. 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 probably be supportive and which of them, whether by choice or because of the situation they are in, might 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 a financial system? For example, what would happen if loans were called in earlier than expected or debtors defaulted?

Financial Risk Governance

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 involve 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, are returns from those which succeed likely to 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 Related 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 into a network could be a kitchen fridge connected to the internet, or an 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 assistance 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? Conformance may be reassuring, but could it reduce vigilance?

What are the advantages and disadvantages of COSO's ERM framework and standards such as ISO 31000? How applicable are they in different situations and contexts? How might they best be used? Could 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 may 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.

■