

Principles of Risk Management for Boards

Brent Wheeler, B.A. Ph.D¹

Introduction

Boards are charged as an implicit if not explicit duty, with managing risk on behalf of their shareholders. The duty arises as a simple corollary of the need to protect, maintain and grow shareholder wealth.

As with other directors' duties risk management should be construed as being concerned with the perspective of the director and governance rather than management. The duty therefore involves taking responsibility and being accountable for ensuring that risk is managed throughout the organisation in a manner which will maintain and grow shareholder wealth as opposed to being involved with day to day risk management practice.

Sources

This paper examines the principles which directors and boards should look to in discharging the risk management duty. It draws on the UK Office of Government Commerce (OGC) methods which in turn rely on international risk standard ISO31000:2009². Further detail is provided by David Hillson/Risk Doctor & Partners at his website <http://www.risk-doctor.com>.

The following interpretation leans toward applications in governance and the perspective from which directors and boards might adopt the principles espoused.

Defining Risk

Perhaps not unexpectedly defining risk turns out to involve complexity. In the present context a reasonably pragmatic approach stressing "steps directors might take" over conceptual elegance is favoured. Essential elements of the working definition adopted below therefore centre on:

1. The fact that it is typically uncertainty rather than risk which boards seek to deal with. Conventionally risk has been defined as the probability of a detrimental event occurring multiplied by the impact of its occurrence. This implies at least some knowledge of the underlying probability distribution which governs occurrence.

More often than not boards and directors have either no such knowledge or only the dimmest perception of the possible probabilities driving the risky outcomes they seek to mitigate. This means boards are for the most part dealing with uncertainty. Stressing this definition cannot in and of itself reduce risk. It can alert directors to the magnitude of the task and breadth of possibilities which adequate responses ought to cover; and,

¹ Executive Chair, The Boardroom Practice Limited

² UK Office of Government Commerce (OGC). 2010. *Management of Risk: Guidance for Practitioners* (third edition). London, UK: The Stationery Office. ISBN [978-0-11-331274-0](https://www.isbn-international.org/number/978-0-11-331274-0)

2. The realms of knowledge available to boards is limited not just by cost but by the intrinsic nature of the knowledge which even could be available. As Rumsfeld D.³ noted, forms of knowledge consist of “the known”, the “known unknown” but most significantly “the unknown unknowns”; the latter concerning issues which are, by definition, not going to be addressed.

Complete mitigation is thus impossible (and given cost considerations likely undesirable). Risk identification, assessment and mitigation therefore concerns the world of judgments and trade-offs rather than certainties and guarantees. Awareness of these intrinsic characteristics of risk is a critical point of departure for boards and directors seeking to manage risk.

Principles

The OGC stresses eight key principles in dealing with risk. These can be elaborated in respect of director and board responsibilities as follows:

1. *Risk management aligns continually with organisational objectives.*

Risk is "uncertainty that matters". What “matters” is any event or out turn which could materially affect achieving the objectives of the organisation. Objectives then, and what affects them, need to be understood thoroughly. That understanding needs to be consensual and shared.

Given such an understanding it is possible for a board to define how much risk is acceptable, and decide how to manage risk within those limits. When either objectives or risk tolerances change, the risk management process and response must change too.

The board’s strategy work (developing, evaluating and monitoring the strategic plan for example) should focus on those risks (and only those risks) which threaten the objectives of the strategic plan. Similarly in hiring and mentoring the CE boards should assess adequacy and performance of the CE against risks relevant to objectives.

2. *Risk management is designed to fit the current context.*

Operations do not take place in a vacuum but occur instead within some sort of external context (for example politics, markets, competition, regulation). This context sets the scene, provides the opportunities and imposes the constraints on the organisation’s internal workings (culture, people and processes).

Risk management efforts must reflect and respond within a context. As context and operating climate change so too must risk management responses from boards and directors.

³ [Transcript of Defense Department Briefing, February 12, 2002](#)

Board monitoring then needs to be directed at ensuring that a continuous link is maintained between risk management efforts in the organisation and the changing context within which it operates.

3. *Risk management engages stakeholders and deals with differing perceptions of risk.*

Different stakeholders see risk differently, and the risk approach must take account of these perceptions. Perceptions may have greater and lesser grounding in empirical reality. Stakeholders may for example hold biased perceptions about both the likelihood of risky events arising and the impact of such events.

Boards need to ensure that bias is recognised and where potentially damaging, that it is countered. Risk management typically involves managing stakeholder expectations regarding risk so as to improve understanding of context and board response to risks.

4. *Risk management provides clear and coherent guidance to stakeholders.*

Achieving clarity is of paramount importance. Clarity means everyone knowing what the risks are and how they are being addressed. Coherence is achieved when risk is understood on a shared basis and managed consistently across all levels of the organisation, and when it is communicated properly across organisational boundaries.

Directors and boards, in bearing responsibility for risk management need therefore to question whether or not and to what extent clarity of purpose is being communicated and how coherent response throughout the organisation is being generated.

5. *Risk management is linked to and informs decision-making across the organisation.*

Boards frequently have to make decisions with incomplete or imperfect information, which makes decisions risky. This may be because of time pressure, the cost of acquiring more information or because an improved quality of information is intrinsically unknowable (for example “the” cure for cancer).

Risk aware decision making is therefore at the heart of adequate risk response. A key management role is to ensure that decisions made throughout the organisation reflect risk.

The best decisions tend to be made when the risks that are associated with different options are understood throughout the organisation. A key board role is to ensure that management drives this end.

6. *Risk management uses historical data and facilitates learning and continual improvement.*

Improvements in risk management can be made by identifying generic sources of risk and developing effective generic responses. History and experience offers valuable lessons. The aim is to become more mature in developing a risk aware culture and risk response practice.

While this behoves management learning and development, directors and boards should incorporate historical experience in strategic plan evaluation and evaluate professional development in the executive in terms of maturity of risk response as part of management monitoring.

Governance structures, rotation policy and induction policies should also reflect the value of continuity and corporate memory in developing increasingly robust risk responses over time.

7. *Risk management creates a culture that recognises uncertainty and supports considered risk-taking.*

Every significant activity involves uncertainty and requires risks to be taken. Success involves taking the right level of risk relative to available mitigation, and balancing risk-taking with reward.

Sustained progress in achieving such risk aware approaches requires a risk-mature culture. Boards and directors should look to CE and management remuneration and assessment structures which reward active risk management, the taking of suitably calculated risks (regardless of outcome since some failure is inevitable where risk is never zero) and the improvement over time in these areas.

Active building of a mature risk culture which seeks out and manages appropriate risk response is a worthy consideration in evaluating strategic plans.

8. *Risk management enables achievement of measurable organisational value.*

The risk management process, seen as a whole, should result in fewer threats turning into needlessly serious problems. It should also help to turn more opportunities into genuine benefits.

Both of these will create measurable value for the organisation through cost avoidance and through allowing potentially risky opportunities to be pursued rather than simply eschewed through fear of unmanaged risk.

Each of these principles presents its own challenges. Moreover developing strong risk response is an on-going process affecting all facets of an organisation's activities. Boards are uniquely placed to adopt objective, organisation wide views which ensure that there is breadth and depth to risk management responses and that a risk aware culture is carefully propagated throughout the organisation. Doing so is a core duty.

Investors are compensated with returns primarily for bearing and managing risk. The survival and growth of their investment depends crucially on risk management. It is therefore incumbent upon their agents – directors and boards – to ensure that taking responsibility for risk appreciation and response to risk is a way of life rather than an isolated category of activity reserved for *ad hoc* treatment on an occasional basis.

The principles espoused above provide one road map toward that objective.