Strategic Risk Governance

an Introduction

David Doughty CDir FIoD FCIM

Chief Executive

Excellencia Limited

Great Western Dockyard

84 Steamship House

Gas Ferry Road

Bristol BS1 6GL

Revised 4 January 2018

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430

Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

Excellencia

bite sized boardroom

Contents

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430

Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

Strategic Risk Governance

Risk in business is inevitable – in fact it is essential. A business which does not take commercial risks will not grow and a business which does not grow is doomed to decline.

Yet, by and large, people in business, as in life, are risk averse, seeking, where possible, to follow the path which provides the lowest perceived risk.

That is not to say that business leaders should behave recklessly, taking unnecessary risks with little regard to the consequences – rather, they should take managed risks and it is the job of the board to ensure that the risks are managed robustly and rigorously.

Businesses need to identify the risks that they face, think of ways in which they might reduce the impact of each risk on the operation of the business and prioritise their focus onto the risks with the highest likelihood of occurrence and the greatest impact to the business.

In so doing, it is useful to group the risks into categories. The following is a list of frequently used categories of risk:

- Strategic
- Operational
- Financial
- People
- Regulatory
- Governance
- Reputational

Strategic Risks are the overarching risks the business takes when it sets or modifies the direction of travel of the business. These risks can be external, when the business is affected by changes in the environment in which it operates or internal risks arising from the adoption of an inappropriate strategy or the setting of unrealistic objectives.

Operational Risks arise from the delivery of the goods or services which the business undertakes.

Financial Risks are to do with the management and flow of the business finances

People Risks are associated with both the employment of staff and, for a charity, the involvement of volunteers.

Regulatory Risks are concerned with the legislative framework within which the business operates.

Governance Risks are to do with the way the business is organised and run.

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

Reputational Risks are any aspects of the activities of the business which would affect its reputation

A good place to start with identifying risks is the Business Plan or overall strategy document for the business.

A useful tool to help to identify risks is an analysis of the strengths and weaknesses of the business and the opportunities available to it and any potential threats to its success.

This analysis can be done at a strategic or operational level within the business to produce a number of items within each quadrant. Sometimes items will appear in more than one quadrant, as a strength can also be a weakness, for example, the involvement of a large number of staff in running a social enterprise is a strength as they are more likely to be engaged with the business, but it can also mean that the decision-making process is longer and less effective than an organisation with a leaner management structure, so it may also be seen as a weakness.

Although when people think of risks they usually focus on the negative aspects – what can go wrong, it is also useful to think of the 'positive' risks presented by opportunities.

Once risks have been identified they can be entered into the risk register so that they can be prioritised and managed.

The risk register is a list of the identified risks faced by the association prioritised in order of likelihood and impact.

It is a tool to enable the board to satisfy itself that the business's risks are being managed effectively and should be viewed on an exception basis, for example always reviewing the top five risks plus those risks which have either increased or decreased in likelihood or impact since the previous review.

Each operating unit or department of the business will also have its own risk register which will feed in to the overall risk register for the company.

The format of a typical risk register is likely to consist of a table with the following headings:

a) Risk Category
b) Risk Description
c) Risk Mitigation
d) Likelihood
e) Impact
f) Ranking
g) Comments

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

The most important elements of the risk register are (b) the description and (c) the mitigation

The risk description should be a clear description of the risk including, where possible, examples to illustrate the nature of the risk, for example:

Risk: Lack of a clear understanding of the market for high-precision widgets

Example: The research department develops a new product which sells in very low numbers and fails to make a return

The risk mitigation is a description of the actions the business is taking and the controls that are in place to minimise or remove the risk, for example:

Mitigation: Regular review of high-precision widget market

Controls: Monitoring of product sales to identify buying trends

At a high-level, the board can use its SWOT analysis to identify and document the strategic risks faced by the business.

For each item in the SWOT table it should be possible to identify one or more risks which are represented by the Strengths, Weaknesses, Opportunities or Threats.

Strengths: Risks in this category are generally those that would reduce the identified strength, making it less of an asset to the organisation. Strengths will provide the organisation with commercial advantages or differentiators to existing competitors or act as barriers to entry to new market entrants.

Organisations never exist in a vacuum and there is always competition, either for the customers or the customer's funds which will seek to erode the advantages and dilute the differentiation.

For each risk there should be one or more measures that will predict the likelihood of the risk becoming a reality and it should also be possible to identify controls which can be put in place or actions which can be taken to mitigate, reduce or remove the risk.

Weaknesses: Having identified the organisation's weaknesses the most logical step is to make plans to strengthen or remove them or reduce the impact that they might have on the business if they continue to remain as weaknesses.

Risks in this category are associated with not making those plans or taking actions to address the weaknesses or any factor which might make the weaknesses worse or increase the negative impact that they might have.

Opportunities: Risks associated with opportunities are mostly associated with the risks of missed opportunities – not being able to capitalise on the organisation's strengths or market position to

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

take opportunities which would advance the achievement of the strategic vision or strengthen the ability to match competitors.

Threats: Threats are those things which might have a negative impact on the performance of the organisation and the risks are to do with failing to mitigate, minimise or remove the threats.

Strategic risks are the risks that either affect or are created by the strategic decisions made by an organisation's board of directors.

Strategic Risk Governance is the set of processes and procedures adopted by the board to ensure that strategic risks are identified and effectively managed to ensure the satisfactory achievement of the board's strategic objectives. It sets out how the board and individual directors can govern strategic risk effectively and equips them with the tools to do so.

A well-developed strategic risk governance framework enables board members to contribute more effectively to strategic decision making and to take a risk-based evaluation of the business's strategic performance

An effective board will also have a Risk Governance Strategy outlining how the board can improve on ways to identify and manage risk issues, and review and update the risk registers for both external and internal risks.

Corporate Governance

Corporate governance is the way an organisation manages its business, determines strategy and objectives and goes about achieving those objectives.

"The purpose of corporate governance is to facilitate effective, entrepreneurial and prudent management that can deliver the long-term success of the company."

(UK Corporate Governance Code)

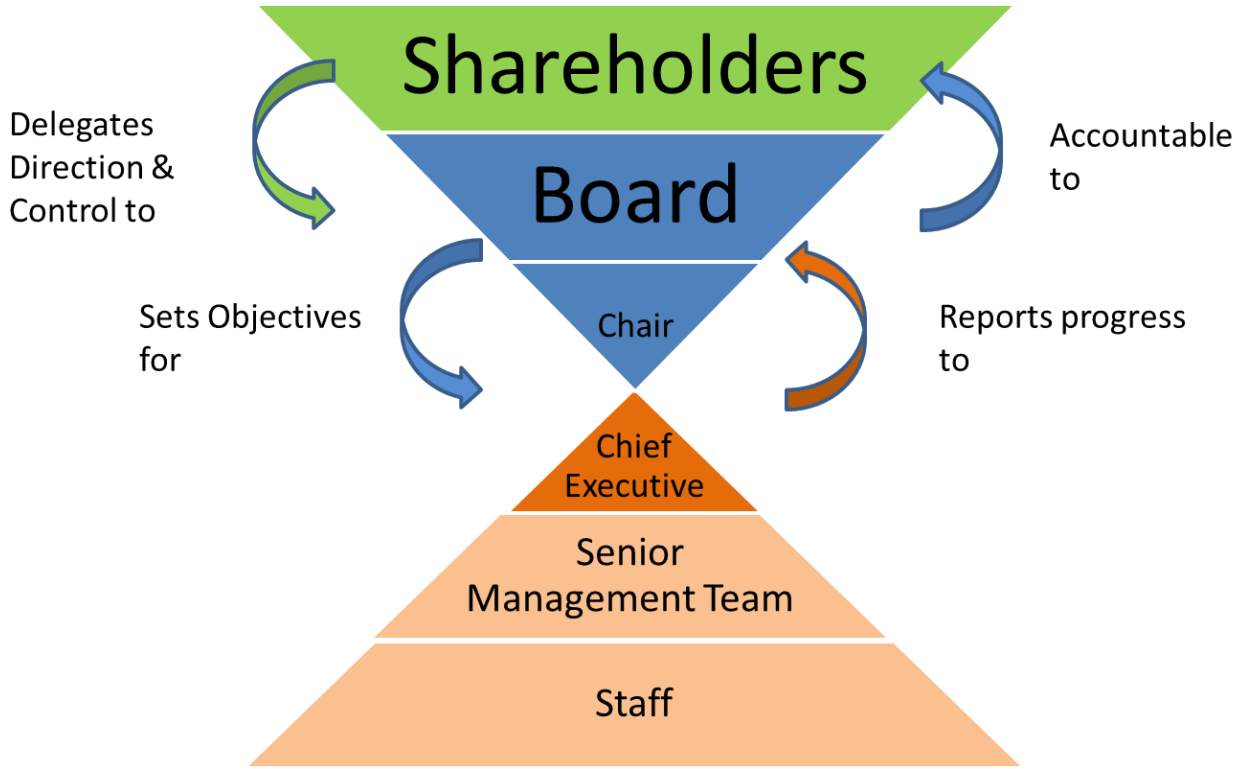
The history of corporate failures shows that governing strategic risks — the existential threats that lie at the heart of the new long-term viability statement under the U.K. Corporate Governance Code — is one of the most important functions a company's board performs. Yet companies too often fail to anticipate these risks, accurately assess them, and/or adequately adapt to them. Collectively, these failures are termed "risk blindness."

As NYU professor Aswath Damodaran has observed, ***"most business disasters can be traced back to bad risk taking...Of all the tasks that make up corporate governance, none is more critical than oversight of risk."***

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

For example, on the basis of an extensive survey, the Travelers 2014 Business Risk Index report concluded that ***"businesses feel least prepared to manage the risks they identify as most serious."*** As Peter Whitehead wrote in the Financial Times, ***"the root cause of most company failure lies in the boardroom, with a serious skills gap and risk blindness being the most common factors."***

A recent McKinsey Quarterly article echoed this point: ***"Boards often overlook existential risks. These are harder to grasp -- all the more so for executives focused on the here and now -- yet harm companies to a far greater extent than more readily identifiable business risks"***. With this in mind, the UK Financial Reporting Council has emphasised that "***boards need to focus especially on those risks capable of undermining the strategy or long-term viability of the company, or damaging its reputation"***



The fundamental basis of corporate governance is that the owners of the business, the shareholders, delegate the direction and control of the business to the board of directors, who, in turn, delegate the day-to-day management of the business to the Chief Executive and the Senior Management team.

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

The role of the board

The key tasks of the board are to:

- Establish and maintain
  - Vision
  - Mission
  - and Values
- Decide strategy and structure
- Delegate to Management
- Account to Shareholders and be responsible to stakeholders

The Board has responsibility for determining the strategic direction of the organisation and for creating the environment and the structures for risk management to operate effectively.

This may be through an executive group, a non-executive committee, an audit committee or such other function that suits the organisation's way of operating and is capable of acting as a 'sponsor' for risk management.

The Board should, as a minimum, consider, in evaluating its system of internal control:

- the nature and extent of downside risks acceptable for the company to bear within its particular business
- the likelihood of such risks becoming a reality
- how unacceptable risks should be managed
- the company's ability to minimise the probability and impact on the business
- the costs and benefits of the risk and control activity undertaken
- the effectiveness of the risk management process
- the risk implications of board decisions

Strategy and Performance

Logically, the variability of performance across firms in an industry must reflect two factors: either some firms have relative competitive advantages, while others do not, and/or some firms make fewer errors than others. In their quest for superior performance and value creating investor returns, management teams and boards spend most of their time searching for new sources of competitive advantage, rather than reducing the frequency and severity of avoidable organisational errors.

Boardroom discussions about strategic risk between directors and management teams are frequently awkward because of the underlying social and cognitive biases

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

at work. Over the course of our evolutionary history, research has found that it has been adaptive to choose as group leaders people who tend to be overoptimistic and overconfident. All of us are also affected by the confirmation bias (the tendency to pay more attention and give more weight to evidence that supports our existing views) and by our natural desire to conform to the views of our group, particularly when uncertainty is high.

The role of the director

In the UK the role of a company director is regulated by the UK Companies Act 2006.

The Act states the seven general duties which all company directors must observe:

- To act within powers
- To promote the success of the company
- To exercise independent judgement
- To exercise reasonable care, skill and diligence
- To avoid conflicts of interest
- Not to accept benefits from third parties
- To declare interest in proposed transaction or arrangement with the company

It is the second of these duties; “To promote the success of the company”, that requires individual company directors to be most cognisant of strategic risk governance.

To promote the success of the company - having regard (amongst other matters) to:

- The likely consequences of any decision in the long term;
- The interests of the company's employees;
- The need to foster the company's business relationships with suppliers, customers and others;
- The impact of the company's operations on the community and the environment;
- The desirability of the company maintaining a reputation for high standards of business conduct; and
- The need to act fairly as between the members of the company

Legal and Fiduciary Responsibilities

The word “Fiduciary” is often misunderstood and used as a synonym for “Financial” – in fact it importantly describes the foundation of company law and corporate governance which is that the company’s directors, as fiduciaries, owe a higher duty

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

of care under law to the shareholders, as principals, than the shareholders themselves as owners of the company.

In recent years, this fiduciary duty to govern risk has become even more important: In a world of greatly increased connectivity, complexity, and uncertainty, skill in avoiding failure has becomes more important than ever before to achieving success and delivering substantial stakeholder returns, because it buys companies the time they need to adapt their strategy in the face of rapid change. As Melanie McLaren, Executive Director of the Financial Reporting Council recently noted, ***"for investors, as providers of risk capital, knowing how the board is managing and mitigating risks is an important indicator when judging whether the company will be able to deliver the value that investors seek."***

Risks

No matter what business an organisation is engaged in, it is exposed to risks. Risk and reward go hand in hand, and the significance of risk to the success or failure of a business is now even greater as technology allows actions and changes to be executed faster than ever before. In the modern world uncertainty has increased, but so have the opportunities for success. To succeed in this environment, directors must be able to manage risks in order that they can achieve their objectives for success. Human nature focuses upon the upside, and expects that the decisions, strategies, projects and operations will go well. No one would suggest that organisations should all become pessimists, but it is becoming increasingly clear that an organisation is much more likely to achieve a successful outcome if it plans and actively manages the risks across the enterprise. Risk management is a fundamental part of the strategic planning and implementation process, and strategic risk management is vital in projects and operations.

Risk can be defined as the combination of the probability of an event and its consequences (ISO/IEC Guide 73).

In all types of undertaking, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside).

Risk Management is increasingly recognised as being concerned with both positive and negative aspects of risk

- What could go wrong?
- How likely is it to happen?
- What would the impact be of it happening?

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

- What should be done to reduce the risk?
- Who owns the risk?
- What else do you need to do about it?

Risk management is a central part of any organisation's strategic management. It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

The focus of good risk management is the identification and treatment of these risks.

Its objective is to add maximum sustainable value to all the activities of the organisation. It marshals the understanding of the potential upside and downside of all those factors which can affect the organisation. It increases the probability of success, and reduces both the probability of failure and the uncertainty of achieving the organisation's overall objectives.

Risk management should be a continuous and developing process which runs throughout the organisation's strategy and the implementation of that strategy. It should address methodically all the risks surrounding the organisation's activities past, present and in particular, in the future.

Risks should be SMART Specific, Measurable, Achievable, Realistic and Time bound

Categories of risk

Categories are widely used to identify sources of risk - some will be of greater concern at the corporate level and some at the operational level, however there is no clear distinction and all levels of management should be concerned, to varying degrees with the majority of categories.

Risk Register

It is good governance for the board to maintain and review its risks assigning a named individual as those responsible and accountable for the management of the identified risk(s).

The risk register is the tool used for capturing important information about the risk or opportunity and is a continual process. New risks will be identified, some will be terminated, and control measures will need to be adapted in response to changing internal and external events or factors. There should be a standard approach to the recording of risks across the organisation.

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

What makes strategic risks different from operational risks?

Operational

Operational risks are inherent in the ongoing activities that are performed across the organisation. These are the risks associated with such things as day to day operational performance of staff, the risk inherent in the products and services and the manner in which core operations and services are delivered.

Project risks - those associated with projects are of a specific, sometimes short-term nature and are frequently associated with the new products or services, significant new research or acquisition, change management, integration, major IT and capital development projects. Project sponsors are accountable for the achievement of project deliverables and outcomes. However, specific risks associated with project management are normally delegated to project managers for attention and action. Included among the benefits of efficiently managing projects are the avoidance of unexpected time and cost overruns. In addition, when project risks are well managed, there are fewer integration problems with assimilating required changes back into general management functions.

Delegated Risks

Whilst the board has ownership of strategic risks it must delegate the other risk categories to management with appropriate assurance mechanisms to ensure adequate levels of oversight. This is a risk in itself as the board is ultimately responsible for the effective management of all risks to the business.

Internal and External Risks

The main difference between internal and external risks is that internal risks can be controlled whereas, for the most part, external risks can only be anticipated or influenced. Strategic risks are predominantly external.

Strategic

Strategic risks are external and internal forces that may have a significant impact on achieving key strategic objectives. The causes of these risks include such things as national and global economies and significantly government policy. Often, they cannot be predicted or monitored through a systematic operational procedure. The lack of advance warning and frequent immediate response required to manage strategic risk mean they are often best identified and monitored by the board as part of their strategic planning and review mechanisms.

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

Identification and Prioritisation

The 5 steps to identifying risks

1. Strategic and Operational Objectives – Vision, Mission and Values
2. Identify what could go wrong
3. Assess - How likely is it to happen? What would the impact be of it happening?
4. Control - What should be done to reduce the risk? Who owns the risk? What else do you need to do about the risk?
5. Monitoring & reviewing - Are the controls effective? Has the risk changed?

Strategic and Operational Objectives – Vision, Mission and Values

The starting point for risk management is a clear understanding of what the organisation is trying to achieve. Risk management is about managing the threats that may hinder delivery of the strategic aims, objectives and operational services, and maximising the opportunities that will help to deliver them. Therefore, effective risk management should be clearly aligned to the following objectives and processes

Identify

It is very important to ensure that the identified risk is a risk to the achievement of the organisation's mission, vision and strategic objectives

Identify the potential risks or opportunities that may arise. Where taking risks that may benefit the organisation, managing these opportunities increases the chance of success and reduces the possibility of failure. By managing opportunities well, the business will be in a better position to provide improved goods and services, better value for money and increased profit.

Each risk needs to be allocated to an owner who will be responsible and lead on the management of that risk, taking forward any action to minimise the risk.

Assess

Having identified the risks it is then necessary to assess which are going to pose the greatest threat or opportunity by looking at both the impact that might result and the likelihood of the risk occurring, producing the overall risk rating.

These scores are not intended to provide precise measurements of risk but to provide a useful basis for identifying vulnerabilities or opportunities, ensuring

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

that any necessary actions are undertaken. The organisation should develop a standard methodology to score risks to help ensure consistent, meaningful scores that can be used to assess risks.

The risk rating needs to be regularly reviewed at strategic and operational level to check that existing controls are effective and to assess any changes should new controls be established, and the risk rating should be amended to reflect changes.

Control

This stage of the process is to decide on a course of action to address the risks identified, to ensure that they do not develop into an issue, where the potential threat is realised. There are four approaches that can be taken to address the risks that have been identified and assessed, these being terminate, transfer, treat and tolerate. Control measures are concerned with the actions taken to reduce the impact or likelihood of risks, not wholly to terminate or transfer.

Monitor and Review

Few risks remain static. New issues and risks are likely to emerge, and existing risks may change. Having identified the risks, assessed them and put control measures in place, it is essential that they are routinely monitored.

Risk management needs to be seen as a continuous process. It is essential that the incidence of risk be reviewed to see whether it has changed over time. Risk Management is a dynamic process which means new risks will be identified, some will be terminated, and control measures will need to be updated in response to changing internal and external events. The assessment of the impact and likelihood will also need to be reviewed in light of management actions.

Monitoring progress and regular reviews provides:

- Assurance that progress is being made towards controlling risks
- Assurance that controls are effective
- Knowledge of any changes to the risk brought about by changing circumstances or business priorities.

When undertaking the monitor and review process, these are the sorts of questions that should be asked:

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

- Are the risks still relevant?
- Has anything occurred that could impact on them?
- Are performance indicators appropriate?
- Are the controls in place effective?
- Have risk scores changed, and if so are they decreasing or increasing?
- If risk profiles are increasing, what further controls might be needed?
- If risk profiles are decreasing, can controls be relaxed?
- How can strategic risk evaluation be improved?

The monitoring and review process should be integrated into existing business processes so that it adds value and supports the successful achievement of objectives and is not just seen as a 'bolt on'. Where objectives have not been achieved or are not on course to be achieved, the cause(s) should be investigated to inform and improve the risk assessment process.

Assurance Framework

The assurance framework is the logical extension of an organisation's risk management procedures. It is a structured means of identifying and mapping the main sources of assurance in an organisation and co-ordinating them effectively. In other words, it is the means by which the board can demonstrate how it knows what it knows about the risks faced by the organisation.

US Secretary of Defence, Donald Rumsfeld, famously identified three categories of "knowns":

- Known knowns – things we know that we know
- Known unknowns – things we know that we don't know
- Unknown unknowns – things we do not know we don't know

For completeness, we can add to that list a fourth "known":

- Unknown knowns – things we don't know but somebody else does.

The board's strategic risk register and associated assurance framework are the physical embodiment of the known known's. They should also highlight areas where resources need to be made available to ensure that unknowns become knowns.

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

Risk Mitigation evaluation

Each identified risk on the risk register should have one or more mitigation statements which outline how the risk is being reduced or eliminated. The board needs to be assured that the mitigation strategies are effective in achieving their objectives in terms of reducing or eliminating risk.

An example of risk mitigation evaluation can be found in business continuity planning where simulation exercises test the organisation's ability to cope with factors which may impact the operation of the business.

By their nature, strategic risks prove most challenging in evaluating the effectiveness of the mitigation processes and procedures.

Risk Governance

Risk Governance is the term which describes the whole process of identifying and managing risks within an organisation. At all levels within the organisation risk management should be a core competency to ensure that the business runs smoothly and effectively.

The board has ultimate oversight of the risk governance process and needs to ensure that the resources, controls, measures and mitigations are in place and regularly reviewed to minimise or eliminate the risks faced by the business in the achievement of its objectives.

Behaviours

Many of the most spectacular company failures in recent years have had their roots in a failed conversation about strategy.

For example, in his book Making it Happen, which describes the failure of the Royal Bank of Scotland, Iain Martin notes how the board conversation about the ultimately fatal decision to acquire ABN Amro moved almost instantly from "Should we do this?" to "Can we do this?"

As Martin relates, an RBS director subsequently rued that the board paid insufficient attention to the critical strategic question of whether the proposed deal made sense.

The behaviours of board members, individually and collectively include a whole slew of natural cognitive biases that surreptitiously drive their individual and collective judgements, such as biases towards optimism, overconfidence, and conformity, as well as the influence of framing and anchoring. These are not flaws in personality or competence of individuals; they are unavoidable human traits.

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

Risk-blindness

Though virtually every involved party was at fault to some degree, bias on multiple fronts was largely the cause of the 2008 financial crisis. Given that bias in risk management can result in a disastrous event such as this one, protecting against biases is critical.

As soon as the financial crisis erupted, the finger-pointing began. Should the blame fall on Wall Street, Main Street or Pennsylvania Avenue? On greedy traders, misguided regulators, sleazy subprime companies, cowardly legislators or clueless homebuyers? Of course, the real answer is: all of the above – and more. Many devils helped bring hell to the economy. And the full story, in all of its complexity and detail, is like the legend of the blind men and the elephant. Almost everyone has missed the big picture. Almost no one has put all the pieces together.

What were the motivations of all the parties? From famous CEOs, cabinet secretaries and politicians to anonymous lenders, borrowers, analysts and Wall Street traders, the crisis was all about human nature.

With warning signs ignored by regulators, financial institutions and academia, the question is, why? Perhaps the answer lies in how human nature manifests itself, with one way being through bias and the groupthink that results from that bias. For example, one view of the cause of the financial crisis is that there were two primary types of bias:

- “Not invented here” bias, which is the unwillingness to adopt an idea because it originates from outsiders, leading to errors in group judgments such as missing out on new opportunities or risks.
- Confirmation bias, which is the tendency to search for, filter or interpret information in a way that confirms existing preconceptions or initial decisions and ignores contrary insights.

Both types of bias contribute to groupthink, in which participants suppress their divergent views in an effort to create consensus.

There are many forms of cognitive bias, including the two above. Other forms of bias were likely involved in spawning and sustaining the crisis (e.g., framing effect, anchoring, belief, availability heuristic, hindsight, outcome and even the ostrich effect, among others). The various forms of bias and the groupthink phenomenon they encourage often result in a desire for harmony in an organisation, meaning

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

greater weight is placed on “getting along” rather than on expressing disagreement on the things that really matter. As a result of efforts to minimise conflict and maximise conformity, a group of this nature tends to avoid critical evaluation of alternative views and salient contrary information and, as a result, reaches risk-reward decisions that may miss the mark badly. In a rapidly changing environment, this behaviour creates lethal “blind spots” in an organisation.

With respect to risk management, bias has always existed. It is not unusual to find evidence of groupthink, dominant personalities, overreliance on numbers, disregard of contrary information, disproportionate weighting of recent events and tendencies toward risk avoidance or risk-taking in any organisation. After all, it is human nature, so, the question is not whether bias exists, but rather how bias within the risk-reward decision-making process can be managed.

As individuals, each of us has our own unique paradigm of how things work based on our past experiences and learnings. Therefore, it is healthy to recognise that biases exist and everyone has them. The following are some thoughts on how to overcome bias in risk management:

- Focus on improving processes rather than blaming people. Most of us have a strong bias to avoid pain, which includes having to admit our failures to others. This is where traders get into trouble: by taking on more risk to cover past accumulated losses, leading to circumstances where they ultimately go rogue. That is why it’s important to focus on the process and encourage people to come forward and escalate issues so they can be addressed in the cool of the day rather than allowed to fester and become a formidable problem with limited remediation opportunities.
- Recognise that risk management inevitably leads to conflict and that it inevitability should be expected and encouraged. Tension is inevitable between value creation and protection. For example, how does an organisation balance its credit policy with its sales strategy? Does a trading operation establish appropriate limit structures when empowering personnel to authorise trades? If prudent public safety considerations are considered to be more important than cost and schedule considerations, how does management know that decisions are being made appropriately across the organisation on matters that could infringe on public safety? The point is that each of these matters leads to dialogue between the independent risk management function and front-line and

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

customer-facing personnel. If risk is to be managed, healthy tension is a good thing. For this to happen, risk management must be positioned properly.

For example, the chief risk officer (CRO) (or equivalent executive) should be viewed by the other executives as a peer and have a direct reporting line to the CEO as well as a reporting line to the board or a committee of the board. Furthermore, directors should conduct mandatory and regularly scheduled executive sessions with the CRO. With the board supporting risk management's independent role within the organisation in this way, the function becomes a viable line of defence.

- When making decisions, reduce the risk of groupthink. It is not unusual for groups to form opinions or make decisions without having engaged in robust debate or listened to dissenting views. That is why efforts should be made to ensure that all views are heard from the right sources and considered. The following are 12 ideas for doing this:
    1. Keep the group a manageable size. Invite the appropriate stakeholders and avoid observers and multiple parties from the same team.
    2. Focus on risks that truly matter (rather than the trivial many). Think about what the organisation doesn't know. Risk assessments directed to cataloguing known risks are not going to generate new insights for management and the board. Focus the company's risk assessments more on circumstances or potential outcomes that have not been considered by the organisation.
    3. Designate a facilitator and do not allow a few to dominate. Be careful about relying on the smartest or most dominant people in the room. Allowing senior managers, experts and dominant personalities to drive what should be a divergent conversation to a point of convergence too soon is a common mistake. Get the facts out and make sure all sides of the issue are voiced, all relevant facts are obtained and everyone whose opinion is valued is heard. Once that is accomplished, initiate the convergence process to a conclusion.
    4. Engage diverse experiences and points of view and avoid "yes people." Diversity in backgrounds and perspectives enriches the dialogue and leads to better decisions.
    5. Avoid starting with a desired outcome or structuring data to fit a preconceived decision. Ultimately, managing risk is about seeking the

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

truth. The earthquake model used by the Japanese nuclear power operator hit by the 2011 tsunami, causing a meltdown of three nuclear reactors, was based on empirical data dating back to 1896; it disregarded important scientific evidence asserting that a major quake had occurred more than 1,000 years ago, resulting in a powerful tsunami that hit many of the same locations as the 2011 disaster did. Geologists had also found evidence of two additional large tsunamis hitting the same region during the past 3,000 years, leading to a view that a catastrophic tsunami was, in effect, a 1,000-year event. While a model based on just over 100 years of data could not possibly offer much insight regarding a 1,000-year event, it certainly supported a conclusion that the nuclear plant's present configuration was satisfactory. Had the additional scientific data been considered or had a different question been asked regarding the consequences of a catastrophic tsunami hitting the plant, the nuclear power operator would have faced the need to consider formidable investment decisions. Geological time is impervious to arbitrary assumptions that ignore the available facts.

6. Distinguish between divergent and convergent dialogues. Recognise when the group is in a divergent mode and when it wants to converge. Remember that divergent thinking leads to better problem solving and more creative solutions. Conversely, convergent thinking shuts down dialogue that is not focused on a single solution.
7. Accept conflict and devil's advocacy as the norm; understand why dissenters disagree. These qualities are the essence of effective brainstorming.
8. Seek diverse external perspectives. From formulating hypotheses to presenting alternative scenarios and their attendant considerations to encouraging healthy debate, management must minimise the impact of bias by encouraging the pursuit of all potentially relevant information, accepting a contrarian voice in the dialogue and, if necessary, seeking diverse opinions from informed third parties. Sometimes, it helps to obtain viewpoints from outside of the organisation. Techniques for viewing the situation in different ways or using different frameworks can be used to minimise groupthink.

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

9. Consider the consequences if a decision is wrong. Management should incorporate the more extreme scenarios into stress tests of financial models supporting critical investment decisions and operating plans. Contingency or exit plans should be explored in case a proposed plan or decision does not work out.
10. Value the differences by looking for synergies in multiple points of view. Recognise the limitations of consensus. In traditional risk maps derived from electronic voting, the collective input of the group is captured in the form of a single point on a grid, as if "consensus" has been reached. However, that point on the grid results from aggregating divergent views. It is possible that one of the divergent views is correct; therefore, the group should determine whether there are outlier views resulting from important information the rest of the group doesn't have.
11. Conduct a pre-mortem. While we can never say with certainty that we know what we don't know, we can apply techniques that encourage managers to think strategically on a comprehensive basis by focusing on the big picture. The "pre-mortem technique" is a process for engaging managers in contrarian, "devil's advocate" thinking without encountering resistance. The idea is to assume that a critical strategic assumption is no longer valid, provide the reason(s) why from a point in time in the future and explain what that development (i.e., an event or a combination of events) might mean to the organisation. Alternatively, more extreme scenarios can be incorporated into stress tests of financial models supporting critical investment decisions and operating plans.
12. We may not be able to identify "black swans" until they happen, but at least we can assess how much they might hurt by considering the cost of being unable to execute aspects of the strategy. If management doesn't like what it sees as a result of this contrarian analysis, steps should be taken to improve early-alert capabilities, contingency plans and response readiness.

- Avoid compromising the quality of your decision-making process. Give the following "don'ts" careful consideration:
    1. Don't structure data to fit a preconceived decision. Ultimately, managing risk is about seeking the truth and acting on it. The aforementioned

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

catastrophic 2011 tsunami event in Japan illustrates what can happen when salient facts are conveniently ignored.

2. Don't rely on the smartest people in the room. As noted earlier, allowing experts and dominant personalities to monopolise the dialogue can stifle the sharing of useful insights.
3. Don't focus on risks everyone knows about. Assessments directed to shuffling known risks around a heat map can't be expected to generate new insights for management and the board. Think about what the organisation doesn't know. Focus the company's risk assessments more on circumstances or potential outcomes that the organisation has not considered.
4. Don't extrapolate the past into the future. Change is not linear. It can be dangerously disruptive. Stuff happens.
5. Don't draw false security from probabilities. Throughout the process, acknowledge that no one can predict the future with certainty. Playing numerology games with probability estimates that are, at best, mere guesses can create a false sense of comfort over "what the numbers say." However, this does not make the threat of a plausible or extreme crisis situation or significant emerging risk scenario go away. That is why a high-impact, high-velocity and high-persistence threat warrants an assessment of an organisation's response readiness. If response readiness is low, a focused response plan may be needed to enhance preparedness.
6. Don't manage toward a singular view of the future. Given the complexity of the business environment, executives should avoid the kind of overconfidence that is often driven by past success. It is common for leaders to make bets based on what they see in the future. But for the big bets that matter, what if they're wrong? "What if" scenario planning and stress testing are tools for evaluating management's "view of the future" by visualizing different future scenarios or events, what their consequences or effects might be and how the organisation can respond to or benefit from them – providing more insight into the hard spots and soft spots in a proposed investment or plan.

While the above ideas are not exhaustive, they suggest that overcoming bias in risk management is all about improving risk-reward decision-making processes

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

continuously so that alternative views are expressed and considered, and relevant facts are placed on the table. Ignoring dissenting viewpoints, suppressing creative thinking and isolating the organisation from outside influences are sure ways for executive management to lose touch with business realities.

Questions for Executives and Boards

Executive management and the board of directors may want to consider the following questions in the context of the nature of the entity's risks inherent in its operations:

- Do we understand the critical assumptions underlying the organisation's strategic, operating and investment plans and evaluate those assumptions with appropriate information from internal and external sources?
- Do we make sufficient use of scenario planning and stress testing to challenge assumptions and expected outcomes, address "what if" questions and identify sensitive external environment factors that should be monitored going forward?
- Are we satisfied that requests for investment funding are presented with a balanced view of rewards and risks?

Risk Identification Techniques – examples

- Brainstorming
- Questionnaires
- Business studies which look at each business process and describe both the internal processes and external factors which can influence those processes
- Industry benchmarking
- Scenario analysis
- Risk assessment workshops
- Incident investigation
- Auditing and inspection
- HAZOP (Hazard & Operability Studies)

Risk Analysis methods and Techniques – examples

Upside risk

- Market survey

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL

- Prospecting
- Test marketing
- Research and Development
- Business impact analysis

Both

- Dependency modelling
- SWOT analysis (Strengths, Weaknesses, Opportunities, Threats)
- Event tree analysis
- Business continuity planning
- BPEST (Business, Political, Economic, Social, Technological) analysis
- Real Option Modelling
- Decision taking under conditions of risk and uncertainty
- Statistical inference
- Measures of central tendency and dispersion
- PESTLE (Political Economic Social Technical Legal Environmental)

Downside risk

- Threat analysis
- Fault tree analysis
- FMEA (Failure Mode & Effect Analysis)

© Copyright 2018 Excellencia Limited Registered in England & Wales number 06522430
Registered Address: 84 Steamship House, Gas Ferry Road, Bristol BS1 6GL