Sue Copeman reports

DEFINITIONS AND

There are a plethora of definitions of enterprise risk management (ERM). Many of them focus on process, rather than looking at what ERM actually seeks to achieve. So AIRMIC recently held a think tank in conjunction with StrategicRISK and sponsored by Strategic Thought to pull together the views of interested associations and see if it was possible to hammer out, firstly, a common definition, and secondly, what participants believed were the hallmarks of an organisation that has successfully implemented ERM.

Introducing the discussion, Paul Hopkin explained that AIRMIC had taken a particular interest in ERM. "We have just commissioned research from DNV into the benefits of risk management, not just to identify those benefits but also to seek to quantify them and then validate that quantification." He circulated various definitions of ERM produced by different organisations, saying: "Some of these definitions simply focus on process: the government bodies tended very much to say 'this is a process', for example. This begs the question, why are we doing that process? A few other definitions actually talk about what you are trying to achieve, and what the outputs should be, such as better decision-making and less disruption to your processes."

Martin O'Donovan commented that treasurers are very conscious of ERM as being wider than the things they have traditionally looked at but probably are not actually doing it to a large extent, although they might be part of a risk committee in their organisation. "ERM is very much an evolving area at the moment."

Richard Feltham, who was not convinced that "we can or should define ERM that clearly, because it means different things to different people" was more concerned about what it results in. "A definition by nature tends to be process-driven and I am more concerned about the outcomes. If we're going to think about definitions, let's think about one that talks about outcomes and benefits, not one that talks in terms of process. How you do it is an individual thing."

Controversially, Lindsay Mercer suggested that some internal auditors may think that the risk management industry has killed risk management as an integral part of management by making it something separate. He felt that any definition should be inclusive and recognise the fact that risk management should not be separate from what professional managers do, but be one of the skills that all managers have and practise.

David Tilston pointed out problems arising from lack of a shared vocabulary. "There is a very real risk of getting hamstrung about vocabulary that people do not understand, and people getting very worked up about definitions and wordings rather than standing back and saying, 'we are trying to manage something, and what do we need to do to limit the variability of outcome?' We should encourage people to be more focused on encouraging people to manage risk rather than worrying about the detail and the definitions." Feltham endorsed this, saying: "If you have a definition, people tend to work within it and it stops people thinking further."

Mark Brown said that strategic thought has often seen a lack of fortitude in terms of driving risk management culture forward across the business. The lack of drive from board level meant that individuals did not have a strong enough remit to make change happen. He concurred that any definition should centre around value.

Also in agreement was Gill Lees: "Regarding people getting hamstrung about definitions, I have been involved with, and seen, people spending a whole afternoon looking at different risks and deciding whether they are operational or strategic and which boxes they should go in. It does not really matter what box a risk is in as long as we have got some understanding of what it feels like and what we are able to do with it."

Establishing risk appetite

Hopkin pointed out here that often the risk register is viewed as the end in itself. Feltham said that one problem was the need to prove that an organisation was 'doing risk management'. "I can turn round and say, 'look at our performance, we've hit all our targets, we've met all our objectives, what other evidence do you want?' But they want to see a risk register, evidence of training and meetings and things like that. Why? We're auditing it the wrong way. Maybe we need to start telling auditors what risk management is about. Until then the auditor and the audit process will drive the bureaucracy."

Back on the subject of a definition, O'Donovan commented: "ERM can mean different things to different people in different organisations as we have said. I suppose a definition gets you started but it is not going to create value."

Brown highlighted the difference between European and US companies. "Larger US companies are concentrating on putting a very thin layer of risk management across the business. Once they've got that and it is consistent, then they look to get to the next level of sophistication in terms of quantification. It's a very different attitude in a lot of European companies, whose managerial sector are trying to do their best but struggle because they don't have the remit to carry out this approach."

Risk management should not be separate from what professional managers do

Mercer considered that a board cannot make a statement on risk appetite in the abstract. "It is not about risk as an isolated concept. It is about things that happen; events that cause results. You give them a list of things that could happen and say, 'These are the results, this is what we are doing and this is how bad it could be. Are we happy with that or do you want to do something else?' If they're not happy, you ask them how much they are prepared to invest to change it by how much. And then you'll get a proper answer."

Lees said that looking at risk appetite in relation to operational issues could produce different risk

PERCEPTIONS

appetites for different areas. Mercer agreed, giving the example of a UK university, which has a number of risk domains such as academic reputation. While it is absolutely intolerant of any damage to its academic reputation, it is far more tolerant in terms of upsetting society and the public, because if it is going to be at the leading edge of academic research it has to run the risk of upsetting people with new and challenging ideas. "What they are doing is giving people guidance on how they feel about different areas so that those people can make decisions based on that general guidance rather than based on any sort of set numbers."

Brown, however, considered that it was important to quantify the cost of various options to mitigate risk, so that the board could make decisions based on the level of investment and the resolution that would be achieved. However, Feltham stressed the danger of making it a purely mathematical calculation: "It takes away that gut feeling, experience and all the other things that make a good risk manager. That's the problem with a definition: there is not that chance to be spontaneous."

Mercer gave the example of a board meeting that was wrestling with a difficult safety problem, where one participant commented: "If that happened, what would we do differently the day afterwards? We need to decide what we would do and then justify why we cannot do that now."

Hopkin suggested that you can look at risk appetite and ERM on three perspectives. "What's our appetite on an operational basis – how much disruption are we willing to put up with? How many people are we willing to kill? And those sorts of operational questions. Then you get into the big project area where risk management is well established and ask, say, 'Have we got the appetite for building a new Wembley Stadium?' And then you get risk management into strategy."

He asked whether organisations get risk management into strategy formulation or whether strategy is developed behind closed doors by the CEO and the CRO who don't want to involve anyone else in those major decisions.

Feltham considered that the way organisations are structured from a governance and a delegated authority point of view sets their risk appetite. "Decisions need to be made at the right level by the right degree of authority and with the right degree of comeuppance if you get it wrong. If you accept the premise that delegation aspects set your appetite, then authority has to flow from the top." To this, Mercer commented: "You haven't got ERM if it does not start at the strategic objective level."

The problem with a definition is there is not the chance to be spontaneous

Brown gave his view. "You may decide as a board not to be compliant with some form of regulation. You can only make that decision by understanding the threats to your business of not being compliant and the opportunities in terms of investment in other areas. Unless you are bring in the whole issue of risk management for governance, compliance and sustainability as part of the definition of ERM, you are missing out one of the key benefits."

Tilston said that, from a board perspective, you have to have some sort of strategic planned broad direction in which you are heading. "Then probably you are going to have a two or three year plan. You have monthly and annual budgets, and you need to make sure that the whole thing is aligned. As part of agreeing the strategic plan, you need to know and have a view on the major risks that you are taking, such as changes in the market, competitive pressures and technology. And you need a continuous check or feedback on that. The board should be weighing up risk on a regular basis with regard to the strategic plan. Most boards will have a formal strategy planning day at least once a year when they'll ask if the strategic plan is still valid, and that's when they might want to change it, probably because their perception of risk has changed."

Hopkin asked whether ERM has to be at a strategic level. He cited the example of a pharmaceutical

company risk manager for whom ERM was an operational issue, all about production continuity. Lees agreed that that was an integral part of it but said that, even so, someone at board level in that pharmaceutical business should be thinking about the future and about strategic risks.

Tilston considered that the board will be looking at the threats to the business without actually mentioning ERM and then communicating any concerns downwards. "Different people are obviously going to be concentrating on different degrees of risk further down the organisation. That is how it is going to happen."

Feltham agreed. "You have to have risk management input at every level at which decisions are taken in the organisation. No one group thinks about ERM; they just think about their own little bit. But it is not ERM unless you have risk management in every level of decision making." Lees pointed out that time horizons expand progressively as you go up the organisation. "So the board should have the longest time horizon down to the person whose time horizon is a day – something has to work on that day."

Brown gave the example of banks. "On trading floors there are real-time credit limits, and automated controls to protect that level of the business, because decisions have to be made in real time. But as you go up through the managerial level, in terms of looking at your value at risk, you move onto a daily view and then a wider time frame. At the managerial level, a lot of organisations have put in some form of risk management for the managers to control and deliver against their responsibilities and are now looking at how they push that down to the operational levels with automated controls."

He added that some of the most risk mature organisations are basically saying that this has to be a bottom up process. Each level of the organisation has its own appetite to absorb and to manage risks and if it can't deal with something it can escalate it to the next level.

Hopkin then asked what were the characteristics of an organisation that does ERM well? "Are they things like risk registers, having board discussions, and having a head of internal audit or a risk manager?"

O'Donovan responded that having people properly trained and skilled in the particular area they are working in would almost be enough in a small company. "In larger companies you need a systematic process, whether that is risk reporting, or risk registers. All kinds of things like techniques, data and statistics need to come into it."

Lees stressed the importance of a culture of resourcefulness. "You want an organisation where there are controls but you also want intelligent people who can take intelligent decisions in the context that they are faced with."

Brown said that large organisations need to put in evidence or incident based processes in order to identify what needs to be changed or controlled. Feltham added that the right controls at the right level give people the freedom to manage.

Mercer was in favour of thinking and doing. He stressed the importance of authorisation – having the retention of a risk approved at the appropriate level. "It starts at the top with the corporate objectives. If you are not thinking about the threats to the achievement of your objectives, you haven't got ERM. But it is not a completely top down process. There should be a conversation where views on those objectives or questions like 'what about this? 'isn't that important?' get raised."

O'Donovan stressed the importance of prioritisation. "Everyone does risk management, but they might be doing the wrong bits, or investing in controlling something which does not really need to be controlled."

Mercer said that a good explanation of ERM was that it was about giving the organisation the best chance of good things happening and the least chance of bad things happening. "You aren't going to eliminate the chance of any bad things happening and you aren't going to get all the good things happening but it is about moving the corporate envelope to get as much of the good stuff in the top right hand corner and as little of the bad stuff in the bottom left hand corner as we can."

Sue Copeman is editor, StrategicRISK

SUMMARY

It was clear from the initial discussion that arriving at an ultimate definition of ERM was not an achievable goal for AIRMIC or indeed perhaps for any of those organisations that have already produced definitions. ERM cannot be defined as a process, and there are too many variables within industries and, indeed, individual companies to produce a 'definitive definition'.

A key problem with reaching a definition is lack of a common vocabulary. There is no point in producing a definition if it means different things to different organisations.

There is also a danger with producing a definition that it encourages people to take a process-driven, tick-box approach. Too close a specification of a very broad concept like ERM might actually limit some organisations, driving them towards a compliance approach rather than actually looking at their own organisation's needs and making ERM fit with them.

However, if ERM cannot be precisely defined, our think tank was far more forthcoming as to its components and the attributes demonstrated by an organisation that has embedded ERM.

So what constitutes a company which has successfully embedded ERM?

- Board commitment and involvement are vital, particularly in giving the remit lower down to make informed decisions on risk.
- Everyone in the company manages risk (although they might not think about what they are doing in those terms) – risk management should be one of the skills that all managers have and practise.
- No jargon – everyone in the organisation has to understand exactly what is expected and the tools they can use.
- Understanding risk appetite for individual risks (rather than just a broad risk appetite concept). Views on individual risks are understandably different, so one size does not fit all.
- Having the necessary information to assess where investment in risk mitigation is going to produce the greatest return.
- Getting and communicating the right decision-making structure so that people know how much authority they have to make a particular decision and can feed questions up if they do not think they are authorised to deal with them.
- Having clearly defined corporate objectives and closely allying risk management to those objectives.
- Understanding the balance between risk and opportunity, measuring where the potential outcome may make it beneficial to take risk.
- Prioritising risk.
- Effective two way – top down, bottom up – communication.
- Measuring risk in such a way that you can identify where several medium scale risks, if they occurred in quick succession, could actually cause a problem.
- Embedding risk management in training so that it becomes second nature for the person doing the job.
- Encouraging intelligent resourcefulness so that people can deal effectively with an immediate risk that they have not been trained to handle.
- Learning from experience – documenting past events and determining how to deal with similar occurrences in the future.
- Avoiding the disconnect that can result in corporate objectives missing some people and a costly concentration on activities that do not reflect corporate objectives.

And above all, having a corporate culture, led from the top, that automatically embraces all of the above!

THE THINK TANK PARTICIPANTS:

Paul Hopkin, technical director, AIRMIC, chaired the discussion
Martin O'Donovan, assistant director, policy and technical area, Association of Corporate Treasurers
Gill Lees, technical department, Chartered Institute of Management Accountants
Lindsay Mercer, representing the Institute of Internal Auditors in the UK and Ireland, who has his own consultancy and has co-authored a number of the IIA's publications on risk management and audit
Richard Feltham, council member, ALARM
David Tilston, education committee, ACT
Mark Brown, chief operating officer, Strategic Thought