Measuring risk committee effectiveness

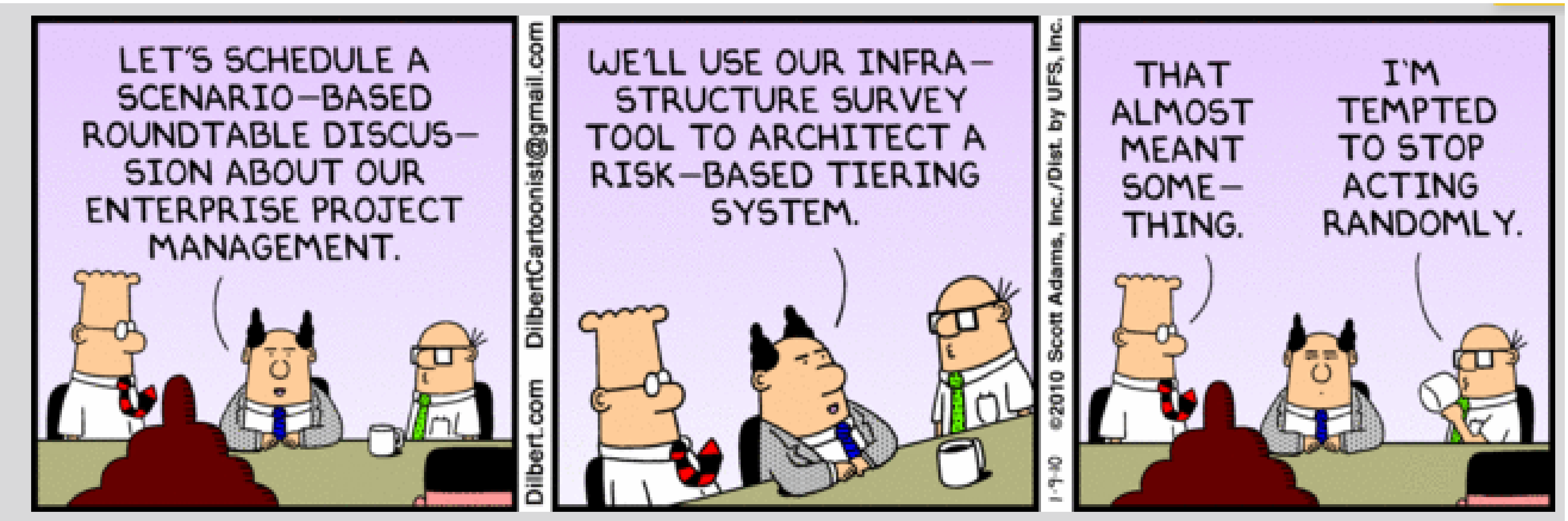
Name: Alex Hindson, Chairman

The Institute of Risk Management

Date: 1st September 2011

Event: ERM SIG

How effectiveness is your risk committee?



How would you know?

What is your risk committee for?

- Terms of Reference of a Risk Committee are key. Is it clear what the committee is meant to be doing?
- Typical Terms of Reference might include:
  - Corporate governance role through challenge and review of risks and their management
  - Setting and monitoring risk appetite and tolerances
  - Establishing a risk management framework as well as policies and procedures
  - Oversight of risk management and internal control systems
  - Receive reports on risk events or external reviews
  - Sponsoring the development of an ERM programme
  - Consideration of new and emerging risks
- It is all providing a structured and transparent framework for governing risk.
- Equally it is about challenging poor practice and driving sustained improvement.
- Risk governance - *"systems, structures, tone and behaviours by which the organisation is directed and controlled, and accountabilities clearly assigned."* has often been overlooked.

What flavour of risk committee do you have?

Committee style and features	Executive Risk Committee	Board Committee	Advisory Group
Key features	Executive led committee with one or more executive directors and functional heads represented	Non-executive led committee with often only non-executive members. Formal Plc Board sub-committee.	Less formal grouping of divisional representatives with risk accountabilities.
Strengths	Clear decision-making and ability to understand key business drivers. Ensures executives are fully briefed on key risk issues prior to engaging with non-executive directors.	Driven by Walker report some financial institutions are adopting this approach to give greater oversight and transparency to stakeholders. Provides more time for consideration of risk issues than available to an audit committee.	Strong engagement from business and focus on practical steps required to manage risks. Very strong at coordinating activities across functions and divisions. Can be used in combination with one of the other two committees.
Weaknesses	These committees often lack senior representation from business divisions who own and manage the risks. This can act as a barrier to embedding risk management.	Ability of non-executives to gain sufficient information and hold executives to account. Potential for conflict with Audit Committee over internal control evaluation.	Can lack the resources and authority to act and be reduced to a talking shop.

Risk Committees – poor relation?

- The effectiveness of Boards has been formally considered for a number of years.
- Section B of the UK Corporate Governance Code issued in 210 restates the principle that “*the board should undertake a formal and rigorous annual evaluation of its own performance and that of its committees and individual directors”.*
- Board sub-committees are coming under scrutiny and it is hardly surprising that Risk Committee effectiveness should be rising the non-executive directors agenda.
- Risk professionals should expect to be come additional scrutiny.
- Additional review should encourage strengthening of corporate governance.

How do I know if it is delivering?

A common structure to evaluating a committee or business process

Summary of current status of implementation and progress versus programme milestones

SWOT analysis

Embedding: Testing progress against Embedding Criteria

'Is this adding value?' Tangible benefits realised to date

Conclusions & Next steps

Level of embedding and criteria	
5	Approaches to managing risk are fully embedded in day-to-day business processes and strategies.
4	Approaches are adopted and improving but not fully embedded.
3	Implementation has been completed in key areas.
2	Implementation is planned but not delivered.
1	There is a level of awareness or understanding but no action has been taken.

1 – Current Status and progress versus plan

- Risk Committees should undertake a self-assessment to determine whether the members feel they are delivering on their ‘Terms of Reference’
- The committee might commission a ‘technical evaluation’ by the risk function
- Example of changes made to committees have included:
  - Establishing a themed agenda for committee meetings
  - Changing the membership to better represent all business divisions and functions
  - Additional meetings to enable the agenda to be covered in full whilst giving papers adequate challenge and review
  - Refocusing papers on covering essential issues and being more succinct
  - Less emphasis (once the committee is established) on process and framework and more discussion of the key risk issues

1 – Technical Evaluation

A technical evaluation might be structured to consider the following for example:

- Committee purpose
- Composition and resourcing
- Teamwork and dynamics
- Agenda and minutes
- Reporting to / from committee
- Risk culture embedding
- Risk appetite and framework effectiveness
- Risk assessment
- Controls and mitigation
- Monitoring and review

2 - SWOT analysis - example

- An honest appraisal of the Strengths and Weaknesses of the committee
  - Level of challenge and scrutiny
  - Structure and robustness of committee operation
  - Tracking of breaches of risk tolerance and driving action
  - Extent to which risk culture is being sponsored
  - Breadth of representation
- An honest appraisal of the Opportunities and Threats of the committee
  - Level of bureaucracy and ‘audit trail’ compared to real discussion
  - Ability of different risk committees (within group and divisions) to communicate effectively within governance structure
  - Clarity of remit of risk committees versus audit committees and Boards

3 - Embedding 'tests' for Risk Management Framework

Test	RMF will be embedded when it is…	Meaning	Score (1 to 5)	Meaning
1	**Sponsored**	Executives understand and communicate the overall framework for managing risks including governance arrangement associated with the Risk Committee.	5	Honest appraisal of risk committee operation against structured 'embedding' criteria. Eg/ to what extend is line management taking ownership of the success of the committee and making decisions.
2	**Owned**	Entity management accept accountability for the risk management framework and how it is implemented locally through the Risk Committee.	4	
3	**Decisive**	The Risk Management Framework ensures that key risk issues (risks versus tolerances, control weaknesses, risk events) are discussed and acted upon in a timely manner.	4	
4	**Commu-nicated**	The RMF is discussed and communicated to staff. Training is provided and awareness information provided to ensure awareness is sustained.	3	
5	**Integrated**	The Risk Management Framework is used to govern all risk and solvency processes via the Risk Committee.	4	
6	**Valued**	The RMF is periodically reviewed and its effectiveness tested. Management look to refine and enhance its implementation over time.	4	
7	**Sustained**	The Risk Management Framework is fully documented and key staff are trained in their respective roles.	2	

4 – How has this process added value?

- Toughest test: - How has the risk committee ‘added value’. In other words what has happened as a result of a having a risk committee, which might not have happened otherwise.
- Examples might include:
  - Challenge of reports and MI (asking the difficult question)
  - Insight (making sense of signals and warnings)
  - Extracting the learning from ‘Risk Events’ reported and ensuring follow up actions are taken
  - Driving adoption of a risk appetite framework
  - Implementing change (eg/ stress test framework, training programmes…)
  - Challenging divisions and functions to adopt and embed risk management practices

5 – Conclusions & Next Steps

- Need to make sense of the findings and draw conclusions.
- It is important that the committee itself makes time to discuss its operation and agree its own action points.
- The review process needs to be owned by the Chair of the committee.
- The actions need to be owned by members of the committee and followed through to completion.

To read more

- Strategic Risk Magazine – December 2010
- Continuity Magazine – March 2011

Assess yourself

When Amlin's head of group risk, **Alex Hindson**, was asked to evaluate his organisation's risk committee, he found a distinct lack of guidance on offer. In the second in our series of practic guides, he explains how you can tell if your risk committee is not delivering

Most organisations have had a risk committee for a number of years, but have they considered whether the committee is delivering any value to the organisation?

Not all risk committees are equal and they come in a variety of different forms. Most common are executive risk committees but there is a growing trend, particularly in banks and insurers, towards the creation of a full board-level sub-committee, on a par with the audit committee. This is largely as a result of the poor performance of risk committees during the financial crisis.

Purpose of the committee

It is wise to reflect on why your organisation has a risk committee and what its role is meant to be. Clearly setting down on paper what the risk committee is meant to do helps to later determine whether it has been successful. But it is surprising how many risk committees do not have a clear remit.

The typical roles and accountabilities of a risk committee could include:

- corporate governance through the challenge and review of risks and their management;
- setting and monitoring risk appetite and tolerances;
- establishing a risk management framework as well as policies and procedures;
- oversight of risk management and internal control systems;
- receiving reports on risk events or external reviews;
- sponsoring the development of an ERM programme; and
- consideration of new and emerging risks.

Board review

The effectiveness of boards has been formally considered for a number of years. Section B of the new UK Corporate Governance Code issued in 2010 restates the principle that "the board should undertake a formal and rigorous annual evaluation of its own performance and that of its committees and individual directors".

In light of the emphasis given to risk management over the last three years, it is hardly surprising that risk committee effectiveness should be high on the agenda of non-executive directors and their advisers. Additional review and oversight should be encouraged as a strengthening of overall corporate governance arrangements.

Self-assessment

The majority of board evaluation is done by self-assessment, with the creation of a questionnaire. Typically, these comprise 15-20 questions, coveri

- committee processes, structure, information a conduct of business;
- business transacted and its relevance;
- committee delegation and reporting processes;
- risk committee member knowledge and skills;
- overall conclusions and free commentary.

Why it's so important

The effectiveness of a risk committee is an importan diagnostic for the health of an organisation's overal risk culture. Risk culture is an issue of increasing interest to regulators and credit rating agencies. This type of exercise if undertaken by a risk functio raises risk professionals' profile in the eyes of senio management, company secretaries and directors. A most importantly, it repositions the risk function a chief player in the overall management and governa of risk issues, not just their technical evaluation.

Alex Hindson is the head of group risk at Amlin plc. He is a fellow and deputy chairman of the Institute of Risk Management

Risk committee types and features

	Executive risk committee	Board committee	Advisory group
Key features	Executive-led committee with one or more executive directors and functional heads represented.	Non-executive-led committee often with only non-executive members.	Less formal grouping of divisional representatives with risk accountabilities.
Strengths	Clear decision-making and ability to understand key business drivers. Ensures executives are fully briefed on key risk issues prior to engaging with non-executive directors.	Driven by Walker Report, some financial institutions are adopting this approach to give greater oversight and transparency to stakeholders. Provides more time for consideration of risk issues than available to an audit committee.	Strong engagement from business and focus on practical steps required to manage risks. Very strong at co-ordinating activities across functions and divisions. Can be used in combination with one of the other two committees.
Weaknesses	These committees often lack senior representation from business divisions who own and manage the risks. This can act as a barrier to embedding risk management.	Ability of non-executives to gain sufficient information and hold executives to account. Potential for conflict with audit committee over internal control evaluation.	Can lack the resources and authority to act and be reduced to a talking shop.

A structured approach

Here is a simple 10-point plan for developing and implementing a risk committee evaluation process.

1. Agree with chairman and committee members a process for committee review.
2. Develop questionnaires and checklists in conjunction with the company secretary or governance function.
3. Issue questionnaires and collect anonymous information.
4. Complete technical benchmarking of risk committee against best practice frameworks, peer organisations or other risk committees in the group (if there are several).
5. Analyse information and identify themes.
6. Communicate themes to chairman and agree proposed conclusions and improvement action.
7. Communicate findings to committee and gain support for findings.
8. Integrate improvements into overall ERM development plan.
9. Communicate the overall conclusions to the bo
10. Track delivery of improvement plans over time and repeat the process.

Can you prove it's embedded?

Alex Hindson looks at embedding business continuity management as a route to creating a risk aware culture and explores the parallels between BCM and ERM

I was motivated to consider the parallels that exist between the key challenges in implementing both business continuity and enterprise risk management having read some very interesting articles in the December copy of Continuity. 'Embedding' is one of those words, like 'enterprise' – everyone uses it, everyone is 'at it', but what does it actually mean?

You cannot turn the page of a continuity or risk magazine without reading about the importance of 'embedding' to the success of any programme. Interestingly working for an insurance organisation faced with meeting Solvency II regulatory requirements, the 'Systems of Governance' requirements under Pillar 2 of these regulations require us to demonstrate 'use and embedding'. This is known as the 'Use Test'. Simply put the regulators are saying, "If you think your models and processes are so good that we should rely on them for regulation, they are good enough for you too; show us how you have embedded them in your decision making." Not surprisingly this is not being focused on by advisory organisations[1].

Is it embedded yet?

I was recently asked by senior executives to come up with a way of measuring 'embeddedness' [sic] across the organisation. My first reaction was, "Great – you have got what this is all about." My second reaction was, "Well surely you know whether it is embedded or not, don't you!" The answer obviously came back "Yes, but can you please prove it, and better still document it for us."

This left me going off into a dark room to think about this more deeply. Having done some digging, debating and benchmarking, I found myself a leading member of the 'Use and Embedding' project workstream, being expected to delivery something workable.

Developing the seven embedding tests

I eventually concluded it would be very hard to come up with tangible measures of embeddedness – it is very much the same problem as measuring a risk culture[2] – but it might be possible to create a series of 'tests' to demonstrate whether it had been achieved. A series of extensive discussions with stakeholders across the organisation resulted in the following 'seven tests' listed in Figure 1.

Test	Is risk management	Meaning
1	Sponsored	Leadership clearly sponsor and challenge activity
2	Owned	Ownership accepted and acted upon at all levels
3	Decisive	Influences key decisions
4	Communicated	Outcomes are visible and actively discussed
5	Integrated	Part of day-to-day core processes and procedures
6	Valued	Pride and commitment drives continuous improvement
7	Sustained	Robust, reproducible and not dependent on single individuals

Figure 1 – The seven embedding 'tests'

What are the embedding tests?

Let's focus more closely on the key elements of the seven tests:

Sponsored – This is all about ensuring that there is executive and board-level support for the programme and this is maintained over time. Leaders should challenge and be demanding, rather than just saying the right things occasionally. Evidence of embedding would include board and management committee minutes, staff magazines, websites and business plans.

Owned – If someone is a 'risk owner', they should positively feel the accountabilities of ownership, and this should be linked to their performance management and reward. This could be evidenced through performance reviews, personal objectives and remuneration committee minutes.

Email: alex.hindson@amlin.co.uk

Tel: +44(0)20 7709 9808
Fax: +44(0)20 7709 0716

Institute of Risk Management
6 Lloyd's Avenue
London
EC3N 3AX
United Kingdom

www.theirm.org

irm

Leading the risk profession