

Embedding risk management and creating a risk culture

Name: Alex Hindson, Chairman

The Institute of Risk Management

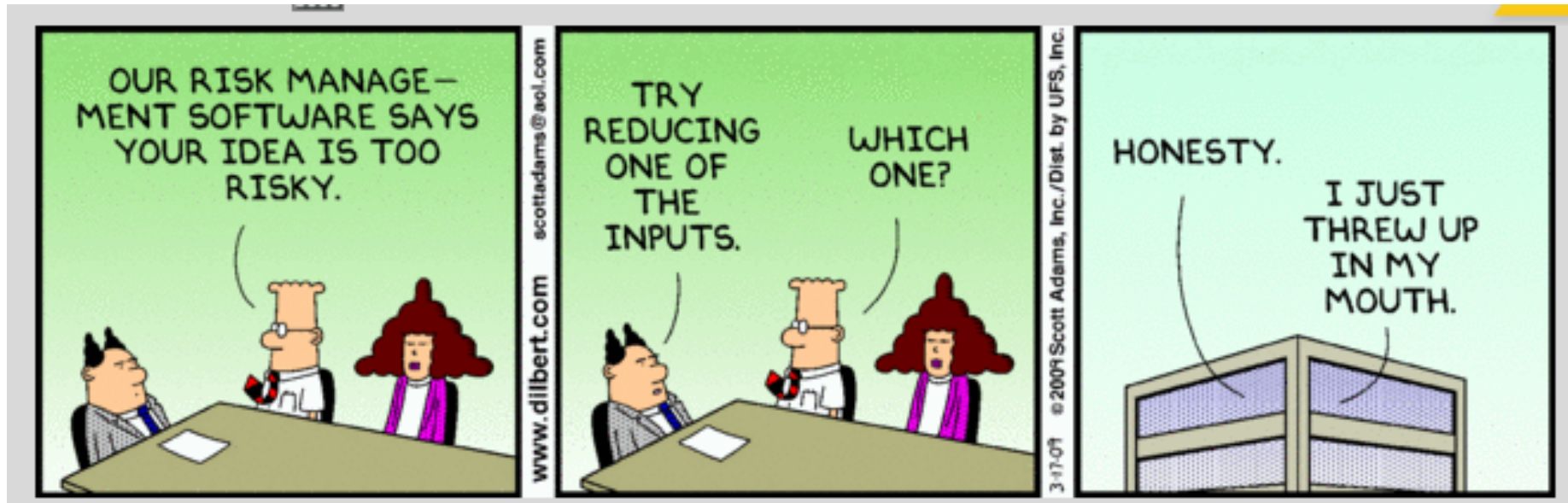
Date: 13 October 2011

Event: IRM Solvency II special interest group meeting

Risk culture – so what is the challenge?



Or alternatively...



What do we mean...

- Embedding
 - Making an intrinsic part of the day-to-day activities of the business
 - Or under Solvency II more accurately...
 - Providing evidence of embedding and demonstrating 'it' is happening
- Risk culture
 - Risk culture is complex and multi-faceted
 - At its simplest it is how 'risk management' is factored into decision making
 - How management is rewarded for taking appropriate risks
 - And how senior management encourage communication on risk and respond to bad news

Risk culture diagnostic

Tone at the Top

- Risk leadership
- Responding to bad news

Governance

- Risk governance
- Risk transparency

Competency

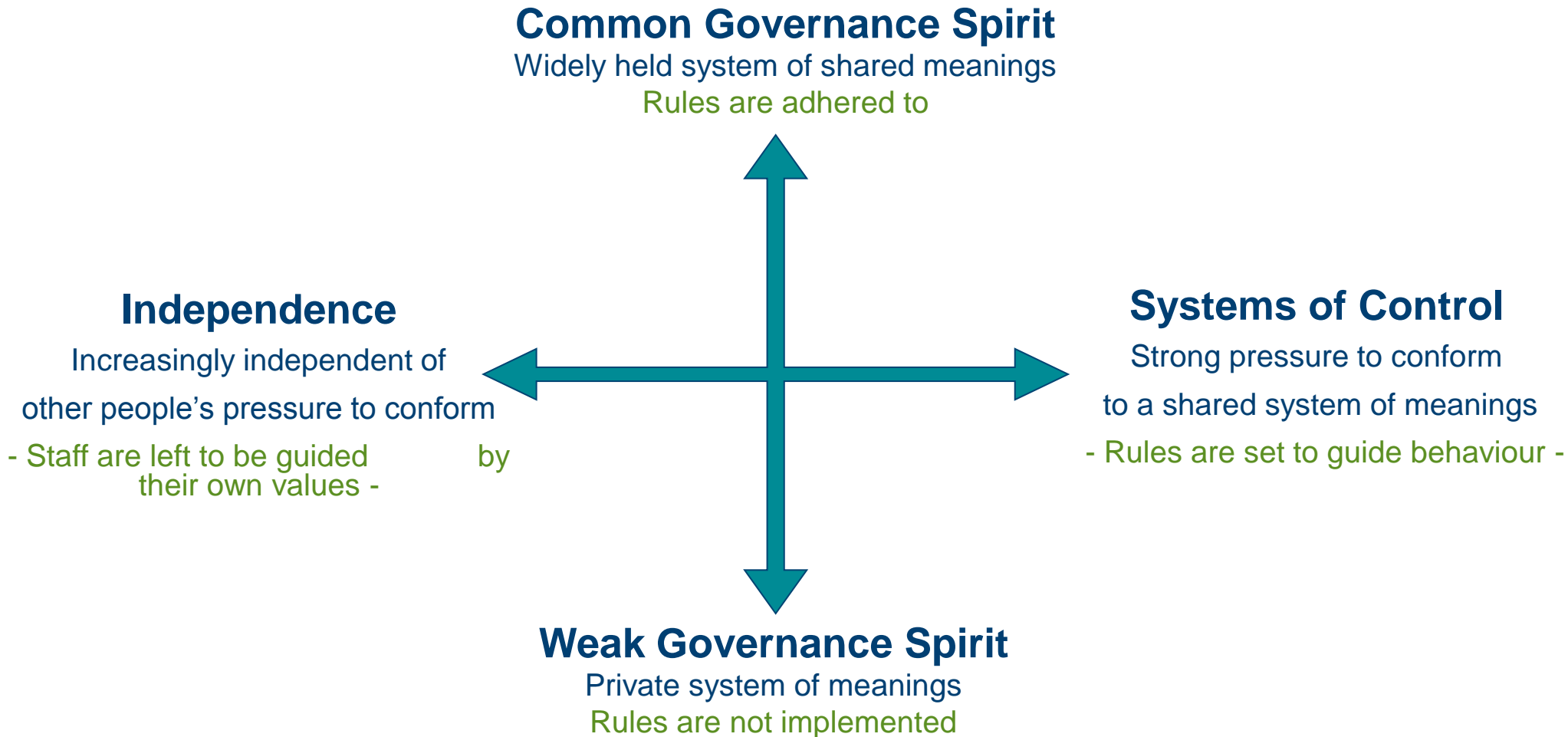
- Risk resources
- Risk competence

Decision Making

- Risk decisions
- Rewarding appropriate risk taking

See article in *Risk Management Professional*

Culture is about shared meanings...



Diagnosing organisational culture

Common Governance Spirit

Widely held system of shared meanings

Rules are adhered to

Engaged Culture Complier Culture

Systems of Control

Strong pressure to conform

to a shared system of meanings
- Rules are set to guide behaviour -

Chaotic Culture

Sleep-walking Culture

Weak Governance Spirit

Private system of meanings

Rules are not implemented

Strategic Governance

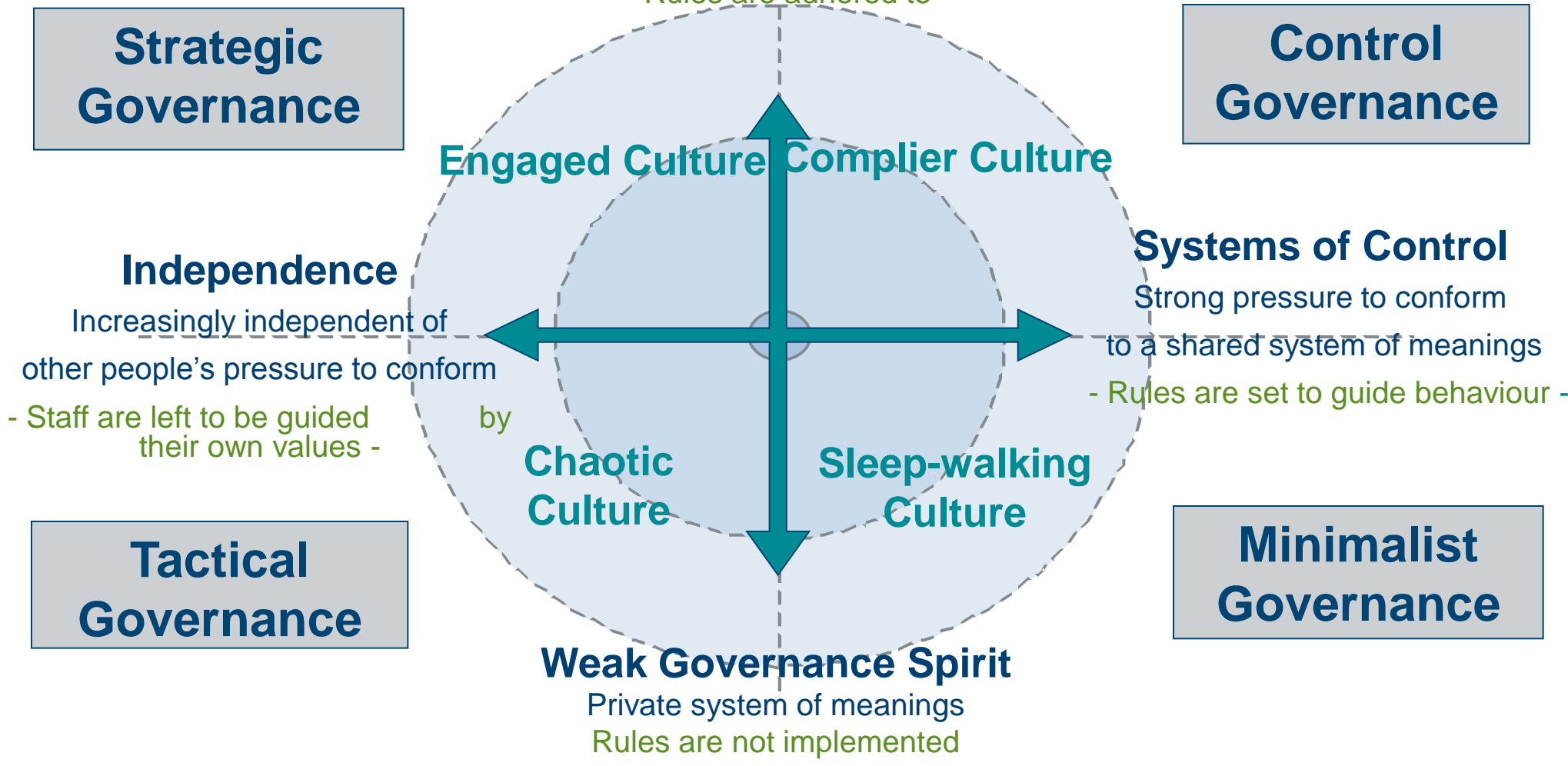
Control Governance

Independence

Increasingly independent of other people's pressure to conform
- Staff are left to be guided by their own values -

Tactical Governance

Minimalist Governance



Style of ERM implementation

Common Governance Spirit

Widely held system of shared meanings

Rules are adhered to

'Sell' Risk Management

'Watch' people comply

Systems of Control

Strong pressure to conform

to a shared system of meanings

- Rules are set to guide behaviour -

'Pray' it works

'Tell' people how to act

Weak Governance Spirit

Private system of meanings

Rules are not implemented

Independence

Increasingly independent of

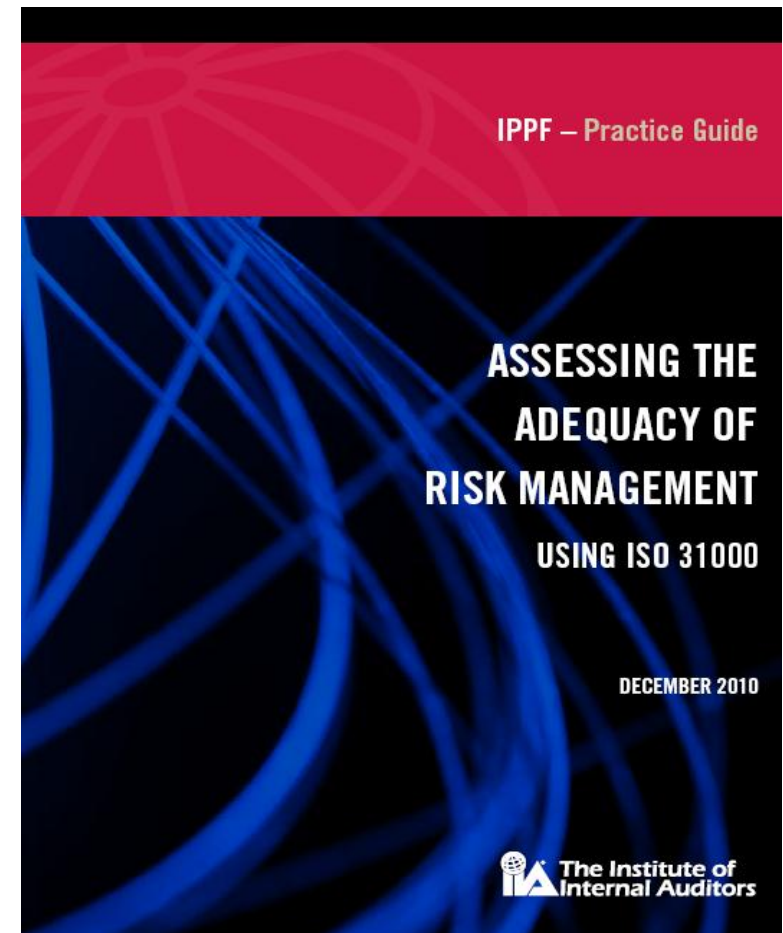
other people's pressure to conform

- Staff are left to be guided by their own values -



Techniques for evaluating risk management embedding

- Need to consider best practice in how to do this practically.
- Institute of Internal Auditors issued a paper December 2010 – “Assessing the adequacy of risk management using ISO 31000.”
- This identifies 3 approaches to providing assurance:
 1. Maturity Model Approach
 2. Process Element Approach
 3. Key Principles Approach



The 7 embedding 'tests'

| 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 |

How to use the embedding tests?

- The 7-tests are extremely simple but very challenging to deliver against
- ‘Baseline’ score each division/ function against key element of a framework or ‘culture tests’
- Identify themes across the organisation and develop improvement plans
- Track progress with periodic re-assessment

| 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. |

Process element approach

- Break the 'journey' into small tangible and measurable deliverables
 - Break it down into activities each quarter
- Define what is most important to your organisation
 - Risk Policy and Standards
 - Risk appetite and tolerances
 - Roles and accountabilities
 - Risk reporting and ORSA
- Put a plan together and get local management buy-in to the activities and timeline
- Track progress and provide support
- Report progress and address issues that arise
- Make it visible and link delivery to local management performance management targets

Process element approach – an example

| Activity | Summary of scope | Entity 1 | Entity 2 | Entity 3 | Entity 4 | Entity 5 | Entity 5 | Entity 6 | Entity 7 | Entity 8 | Target end 2010 | Target end 2011 | Average |
|---|---|----------|----------|----------|----------|----------|----------|----------|----------|----------|-----------------|-----------------|---------|
| Risk Strategy | Risk Management Framework understood & communicated. Policy direction championed actively. | 3 | 3 | 2 | 2 | 3 | 2 | 3 | 2 | 3 | 3 | 4 | 2.5 |
| Risk Standards | Risk Standards are adopted, gap analysis completed and improvement plan agreed. | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 4 | 2.0 |
| Risk Appetite & Tolerances | Risk appetites and tolerances are agreed and risks are monitored against these. | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 2.7 |
| Accountabilities and Ownership | Accountabilities within the risk process are understood, agreed and acted upon. | 3 | 3 | 3 | 2 | 4 | 2 | 3 | 3 | 3 | 3 | 4 | 2.9 |
| Risk identification & assessment | Risks are proactively identified, discussed and evaluated using the risk system to capture conclusions. | 3 | 2 | 2 | 2 | 4 | 3 | 2 | 2 | 2 | 3 | 4 | 2.5 |
| Risk Response | Improvement plans are agreed and acted upon where necessary to address deficiencies or risk events. | 3 | 2 | 2 | 2 | 2 | 1 | 3 | 2 | 2 | 3 | 4 | 2.0 |
| Risk Reporting | Risks, including emerging risks and risk events are proactively reported by coordinators with limited input from the risk function. | 2 | 2 | 1 | 1 | 3 | 2 | 3 | 3 | 2 | 3 | 4 | 2.1 |
| Risk Review & Governance | Governance arrangements are clearly defined and acted upon. Management and Boards review & challenge risk data. | 3 | 3 | 1 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 2.7 |
| | Average | 2.8 | 2.5 | 1.9 | 1.9 | 3.0 | 2.3 | 2.8 | 2.5 | 2.5 | 3.0 | 4.0 | 2.4 |

How this approach can be deployed

- Practical experience suggests it works well if...
- Local management take accountability for progress reporting
 - Make local management report their ‘embeddedness’ with evidence (Its only embedded if they say so...)
 - Instil some competition between areas
- Can we used to evaluate a division’s progress or evaluate specific processes
 - Risk committee effectiveness
 - Risk Assessment and emerging risks
 - Risk event reporting and stress testing
 - ORSA process development

Its about more than just process and evidence

- Integrating with Learning & Development programmes -



The flyer is for a course titled "Managing Risk" by Amlin Academy. It features the Amlin logo in the top right and the Amlin Academy logo in the top left. The text reads: "We are all Risk managers! But do we understand what this means?!" followed by "A one day course on the fundamentals of Risk Management. This new course on Risk Management – a combination of theory and simulation – will help you understand what risk means to Amlin, the range of risks we face as an organisation and how we all play a part in managing these uncertainties." Below this, it says: "Whether you are new to Amlin, involved in the Risk Management process or are simply interested to know more about Risk Management, this course will provide you with the fundamentals of Risk Management including terminology, and the basics of the risk management process followed at Amlin." At the bottom, it says "For more information please visit the [AMLINACADEMY](#)". The flyer also features a photograph of three people (two men and one woman) working together on a wooden structure, with the words "Teamwork", "Energetic", and "Educational" written around the photo. The word "Practical" is written above the photo and "Interactive" is written to the right of the photo.

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



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'.

Is it embedded yet?

I was recently asked by senior executives to come up with a way of measuring 'embeddedness' '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 deliver 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 – 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.

Continuity magazine March 2011