The Effective Board

INDEPENDENT AUDIT
BOARD REVIEW

January 2017

Is your risk management *truly* effective?

RISK MANAGEMENT EFFECTIVENESS
EVERYBODY HAS ONE –OURS LOOKS THE SAME
WE'VE HAD IT A LONG TIME
PEOPLE FOLLOW IT
THEY'VE STOPPED COMPLAINING
THE AUDITORS SAY IT'S OK
PENWILL

You'll most likely have in place an "enterprise risk management" system. Most of you will have had one for years – and over that time the business will have spent quite a bit of time and money on getting it in place and keeping it alive. And you'll probably be feeling that it's most likely working OK as it looks and feels like every other risk management system that you've seen elsewhere: if everybody's got one, it can't be far wrong.

But as a board member, you wouldn't be at all unusual if you had a nagging doubt that there might be something missing. Is our risk management really having the impact we want? Has it really got traction in the business? Does it really help us make better decisions? Why are things still going wrong even when we'd identified them? Or why didn't we spot them coming? And anyway, it's what the risk management consultants and the various bits of guidance say you need to have.

Now is the time of year when many boards have to say something about the effectiveness of their risk management and control. So it might be a good time for the board – or at least the Audit/Risk Committee – to stand back a bit and think through how it's judging "effectiveness". We have plenty of ideas on what needs to happen and what shouldn't – here are just a few.

Good practices to consider...	Things to avoid...
Work out what you mean by "effective". We think it should mean looking at the impact on the business: does risk management help better decision-making and result in better outcomes? Does risk management activity lead to better business management? That can be difficult to judge – but at least it's a good starting point.	Assuming that, because you have well-established and a recognisable risk management process in place, it's effective. It may not be doing any harm (although there is a danger of false reliance) and it will most likely be doing some good (so we're not suggesting it's a waste of time and should be ditched). But that doesn't automatically mean it's effective in helping the business perform better.
Make sure that what you expect from your risk management is clear – with a consistent message coming from the board and executive. Does the business really understand the purpose, importance and value – in other words, why it matters? For that to happen, the board and executive need to have a clear idea themselves of the value… and share that conviction with others.	Thinking that the value of risk management should be blindingly obvious to everybody. Some will see it as an imposed process which only merits a tick in the box. Others will see it as a vaguely useful exercise but one which is just putting some structure around what they do anyway. If you want it to stick, you have to try to think through the different mindsets and address them with a clear message.

Good practices to consider…	Things to avoid…
Tie risk management objectives into the strategic context. So, for the full board, that means setting out what we really need to get right to achieve those objectives, what needs to happen to make it go right, and what might stop it. For the committee it means following that through to its assessment of how those risks are being managed, with a strong emphasis on what really needs to go well.	Coming up with a list of "principal risks" that, at least in part, isn't connected with what we must get right if we are to succeed. How far do the risks tie in to the core drivers of performance? Can you answer the question "how will this list help us to lead the business towards success better than we would otherwise do?" And then, of course, there's always the possibility that management can't put the assessment into a strategic context because they're not sure what the strategy is… Now *that's* a risk.
Try to restrict the contents of the principal risks list to things which are actually risks rather than theoretical or highly improbable scenarios. The actual risks include things like uncertainties where significantly different outcomes are possible; threats that are starting to emerge in the outside world; stresses and strains building up in the organisation. All are things that either you can do something about or you can prepare for by ensuring resilience in the organisation.	Avoid including so-called "risks" which are not best handled by risk mitigation. "Our strategy might be inappropriate" is certainly something to avoid but the answer is to work on the strategy to ensure it isn't, not to record the fact that there is a strategic planning process. "Customers might stop liking our products" would certainly be disagreeable but it's not something you manage by including a few sentences in the mitigation column of a brightly-coloured spreadsheet. And things which have already gone wrong are not risks, they are facts.
Set out the intention of risk management and how it should work, in a structured, documented Risk Management Framework, signed off after careful review by the committee, if not the full board. Looking at structures, responsibilities, resources, linkage to strategy and appetite, tie-in to reporting… this should set out what needs to happen to help make sure that risk management has an impact on the business.	Adopting a Framework that simply sets out agreed processes without tying it into objectives and how it really needs to work in this particular business. Or not adopting a Framework at all, relying on piecemeal polices and processes. It's up to the Audit (Risk) Committee to make sure the framework is compiled by management, is relevant and is communicated as a living document and tool, not becoming an optional "leave on the shelf" point of reference.
Think through the behavioural angle: what attitudes and behaviours do we need to see sustained to support strong risk management and internal control? That means working out how to assess those attitudes, looking at, for example, how people respond to the risk management processes, how risk-taking and values are linked, how people communicate, the level of acceptance of the risk appetite…to highlight just a few.	Assuming that, just because a well-designed process is in place and people have been told to follow it, that they'll do just that. There are many different factors in how people respond to a required process but the bottom line is – if it's useful, it's much more likely to get done. So assessing opinions and working out how people are relating to the risk management processes and standards is a key aspect of working out whether risk management is effective.
Look closely at the management monitoring. It's well-accepted that risk management should happen at the operational level. But that needs following through by looking at how risk management performance is assessed as part of operational processes. That means looking at factors such as monitoring versus appetite, focusing on change and emerging risks, keeping an eye on "business as usual" risks, analysing root causes…	Approaching the "risk management assessment" by limiting it to the risk management processes overseen by the risk function. It goes much wider than that of course, with a core component being the "first line" activity and the "second line" management oversight. The committee's assessment needs to include looking at how risk assessment is built into first line processes and management.

Good practices to consider...

Assess what actually happened. What went wrong in stopping us achieving a strategic objective? Was it under-performance or did a risk crystalise? And if it did, was it identified and how did we set out to manage it? And that applies across performance targets, strategic initiatives, Business As Usual, projects…

Things to avoid...

Neglecting to learn from events. It might be tempting, or a natural inclination, to look forward with an attitude of "what's done is done". But that's not the best way of reducing the risk if it happens again. A strong learning organisation will consistently assess where things went wrong. And an audit(risk) committee should be active in helping make sure this happens. It's all part of effective risk management, so how well it's done needs to be assessed an as integral part of the process, not as a "nice to have" when people remember to do it.

HOLD THE DATE - RISK MANAGEMENT WEBINAR

Our next webinar on Tuesday 28 March 2017 will be on how audit(risk) committees can take a more structured approach to assessing the effectiveness of risk management.

Click here to register your interest

Thinking Board®, our online self-assessment tool, gives you online access to our knowledge and experience. We now have available a special module designed to help assess the effectiveness of risk management.

Find out more

INDEPENDENT AUDIT

Independent Audit are leading specialists in governance, risk and assurance. We help clients understand and improve the effectiveness of their governance, including the board and its committees, internal and external audit, and risk governance.

If you have any questions on the issues covered here, please contact Richard Sheath at richard.sheath@independentaudit.com

This eBulletin is published monthly. To see back issues click here: "The Effective Board".

To subscribe click here

www.independentaudit.com
+44 (0)20 7220 6580

INDEPENDENT AUDIT
BOARD REVIEW