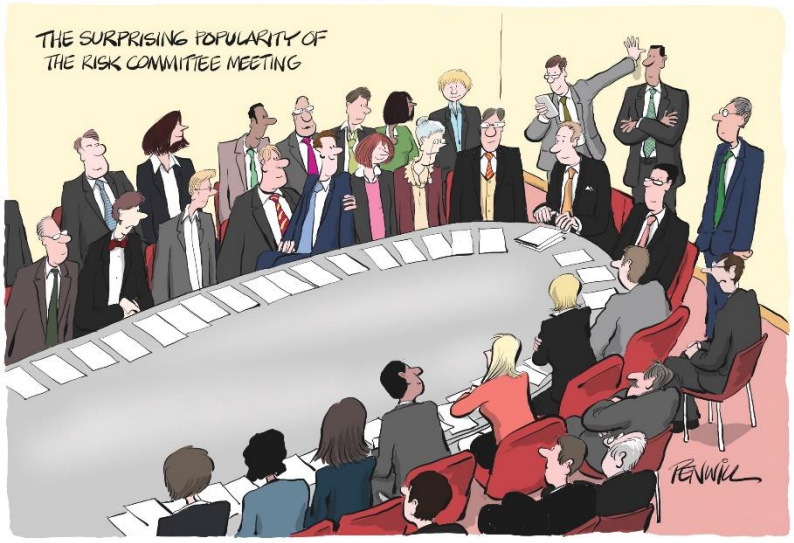
The Effective Board

INDEPENDENT AUDIT
BOARD REVIEW

May 2017

Committees and Risk

Dealing with risk at the board committee level can be a tricky business. The intimacy of the relationship between risk and strategy makes getting the focus right quite complex. With risk committees now standard for regulated financial institutions – and regulatory expectations of their work ever-increasing – the complexity becomes all the greater. And, even where oversight responsibility is still sitting with the Audit Committee (still the case for most non-financial services businesses), many of the same questions about their approach and scope of coverage apply.



There isn't a set of "one size fits all" rules that should be applied: boards need to make sure that the committees work well in the context of their business. But, in pinning down how the committee should work, there are some common questions that should be considered – along with some unhealthy practices to keep an eye out for.

Good practices to consider...	Things to avoid...
Be sensitive to discussions of risk exposures becoming strategic questions. There are numerous angles to consider. If it's a matter of deciding to accept major risks or reduce exposures, is it a strategic matter? If so, are the right people in the room and is the right person in the chair? Are the meeting dynamics what's needed for a strategic discussion? Is the level of formality in line with that of a board meeting? Has the question been properly prepared? Is it being considered in the overall strategic context – and tied into the board's risk appetite?	Allowing risk committee meetings to become, in part, board meetings. That happens when discussions on risk exposures drift into strategic "risk acceptance" decision-making, particularly when the approach becomes "we're all here anyway so we might as well discuss it now rather than again at the board". Whilst pragmatism needs to be applied, at the same time there needs to be a constant awareness that full board meetings are different and are the right forum for strategic decision-making. The committee chairman needs to be very alert to the need to defer at least part of the discussion – and, for certain, any decisions – to the board meeting.
To help maintain this sensitivity, try to keep in mind a distinction between "risk acceptance" and "oversight of risk management". "Acceptance" discussions could become strategic in nature – whereas detailed oversight of risk management processes fall squarely within the committee's remit (whilst nonetheless recognising that ultimately the full board has responsibility for the effectiveness of risk management).	Assuming that anything containing the word "risk" falls within the risk committee's remit. Inevitably, a committee has to review risk exposures in order to assess the adequacy of the risk response. But there's a difference between assessing the level of exposure and the way it's being managed, and making a decision that it's strategically acceptable.
Keep the "risk appetite" front of mind. If the full board has agreed the risk appetite, then the committee can assess exposures versus appetite in those risk areas without worrying so much about drifting into strategic decision-making.	Going through "risk appetite" setting at the board level – and then not doing anything with it for the rest of the year. Imperfect though the concept of risk appetite might be, it can still be useful in helping the committee assess how far the risk exposure is in line with the board's intentions and as a way of tracking developments against a fixed point.

Good practices to consider...	Things to avoid...
Help the board get to a useful definition of principal risks and risk appetite by doing some of the heavy lifting beforehand. A lot of thinking and discussion is needed – more than is usually possible within the constraints of a board meeting. This includes making sure that risk appetite is a relevant concept for each of the risk areas being considered. Just be careful not to stray into board discussions: the committee should be acting as the pre-meeting "sherpa".	Thinking that simply leaving the principal risk and appetite discussion to an hour's slot each in the occasional board meeting (if that) will be enough. It might be – but only if the committee has worked with management in setting out beforehand the issues, options, analysis, implications.... It also needs to set these out clearly for the board, ideally in a well-structured paper – so that means doing it a few weeks ahead, not the day before the board meeting.
Make sure that the committee gives plenty of time to understanding how the risk management framework is supposed to work – and how it is actually working. And that will mean getting down into the detail, whatever the nature of risk.	Losing sight of the core responsibility of the risk committee to look at the effectiveness of risk management processes, structures and systems. It's probably more interesting to look at the exposures and how much risk to take, but the agendas and discussions need to keep the right balance and not tilt unduly towards the more engaging topics.
Develop a clear view of what you mean by "effective" risk management and how you are going to assess it. That probably means adopting a model so that you can think through the different influences and activities that make up "risk management" across the business.	Thinking that "risk management effectiveness" is all about processes and structure. That's part of it – but risk management is only effective if it's having the desired impact. So, you need also to look well beyond the process and look at the strategic direction given to risk management, the behavioural angles ("risk culture"), management monitoring – and what actually happened and how lessons are learnt.
The changes to the Code and Guidance in 2015 had a clear intent (even if the wording was less clear): committees are expected to be more active in assessing risk management on a regular and continuing basis.	Thinking that we're still working along the lines of "Turnbull statements". That annual review was never particularly effective in encouraging a close look at how well risk management is working and soon lapsed into inevitably positive boilerplate statements, often "evidenced" by unconvincing effectiveness reviews. Much more is now expected – especially from regulated entities.
Be demanding when it comes to risk reports to the committee. Make it clear what questions you want to have answered and how you want the information set out. Demand opinion and assessment – not just heat maps and summarised risk registers. And if you feel the picture is getting buried by the detail – make sure you keep asking for changes until you get what you need..	"Losing the will to live" when it comes to risk reports. Whether that's when you're actually trying to get through the report and working out what it's trying to communicate (or even trying to read it at all, when the font is so small and the "information" so crammed on to the page). Or whether you feel you've asked so many times for less detail and more evaluation and still aren't there – but opt for the line of least resistance by accepting something you're still not happy with.
Ensure that the agenda, and the risk reporting, allow you to focus on the big picture. You should be able to leave the meeting with a sense of "how thin is the ice on which we are skating" and confidence that sensible things are being done to prevent things going badly wrong.	Allowing the risk discussion to be dominated by discussion of "risk issues", a popular euphemism for "something that has already gone wrong". Yes, problems need to be addressed. But it's even more important to spend time on how the likelihood of future problems is to be reduced. Learning from past problems in order to avoid repetition is important, but not enough.

Good practices to consider...	Things to avoid...
Regularly assess whether you have the right people in the room to answer the committee's questions. The committee's oversight means holding the people responsible to account for managing the risks to the desired level – through a combination of good decisions and following policies and processes. So you need to speak to the people responsible for running the business, rather than having everything intermediated by control functions.	Just engaging with the Second and Third Lines. They are not the ones ultimately responsible for risk taking and risk management. Yes they have important roles in the risk management framework and need to be held accountable for their performance of those responsibilities. But to understand the reality of how the business is managing risk, you need to speak directly to management – so, bring them into the room from time to time to look them in the eye and hear first-hand about what's happening.
Strike a balance. Since risk touches the entire business, having the right people in the room could mean having everybody, or at least most of the executive and supporting functions – and it's hard to have a clearly focused discussion with too many people. If the purpose and scope of the risk discussion is clearly defined, it should be possible to have the right people present and still have room to breathe.	Opening the meeting to all-comers. Sometimes it's a compliment – the discussion is really getting into meaty issues. But sometimes it's because executives feel the need to keep an eye on what the NEDs are up to. Or, more creditably but equally unhelpfully, because the meeting is always allowed to drift into interesting discussion about business issues and this is a good opportunity for executives to get together to discuss them.
Make sure the Head of Internal Audit is at the meeting – for the duration. If you have a separate Risk Committee, make sure the HIA is there to answer questions about controls, risk management processes and effectives, what happened when things went wrong, "culture" and attitudes… the many things they pick up throughout their audit work. And of course Internal Audit needs a full understanding of the board's risk appetite if they are properly to judge the significance of audit findings. They'll get this much better from listening to the committee's discussions than from anything written down.	Leaving them out because they're responsible to the Audit Committee. Yes, that's the primary reporting line but the Head of Audit will (or should) have a lot of insight to share. Operational risk is largely mitigated by internal controls and that's Internal Audit's territory. So, in the same way that it's common for the risk committee and the audit committee chairmen to sit on each other's committee in order to minimise the risk of confusion over the boundaries, the HIA and the CRO should also cross over.
Consider inviting the external audit partner to the risk committee meetings. All the audit firms use risk-based audit approaches, so the auditors ought to find the discussion useful. And if they know the business well they might have something to contribute.	Assuming that auditors only belong to meetings, or parts of meetings, that contain the word "audit" in their title. There can be good reasons why risk committee discussions aren't relevant to the auditors – but there are also bad reasons, such as the auditors not being sufficiently interested in the business and its risks, or the meeting discussion being too anecdotal.

What's new...

Risk Reboot

Boards are starting to think it's time to take a fresh look at how risks are managed. They are asking how far does their risk management really helps them make better decisions and get things right?

Independent Audit Limited and Hans-Kristian (H-K) Bryn have collaborated to develop a new proposition – Risk Reboot – to help boards and executive committees really understand how risk management will help them manage future uncertainties…

Assessing... Risk Management Effectiveness

Risk management is working well when it when it helps you run the business better. In assessing effectiveness, that's what you need to look at. But too often the focus is on the process.

The Independent Audit Risk Management Effectiveness Model powered by Thinking Board®, our governance self-assessment tool, shifts the focus – and your thinking… register here for your free risk management demo.

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 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