The Effective Board

INDEPENDENT AUDIT
BOARD REVIEW

October 2017

(Audit and) Risk Committees

Since the advent of Risk Committees following The Crash, boards haven't always found it easy to make these things work well. (By the way, whether you've got a separate risk committee or not, don't think you can stop reading now – this Bulletin still applies to you! And for "risk committee" below read the committee overseeing risk management. If you just have an Audit Committee, its responsibilities around risk management are likely to be – or should be – just the same as a board with a separate risk committee.)

THE COMMITTEE TACKLES THE RISK REGISTER

What gets covered and how can be unclear: there are quite a few fuzzy lines meaning a lot more "about risk" can end up in the Committee's lap than might be right. And some careful thinking is needed around attendance and how the committee works – especially the way management report. So here are a few pointers as to what to think through and possible traps to avoid.

Good practices to consider...

Define clearly which responsibilities sit with the full Board and the board meeting – and which with the committee. It's clear that assessing the effectiveness of internal control and risk management is a committee responsibility. But when it comes to assessing risks and the acceptability of risk exposures it's less clear. As a rule of thumb though, the Board should be responsible for risk strategy (appetite), overall risk policy and framework – and any exposure that is (or could become) particularly big or ugly.

Things to avoid...

The committee's assessment of risk exposures morphing into a discussion and decision on whether or not it's acceptable to maintain that exposure or overall risk profile. Yes, the committee will want to look at the risk exposures otherwise it can't judge how they need to be managed. But, at least for the big exposures, the decision as to whether they are acceptable should probably be a full board discussion in a board meeting – unless the risk appetite has clearly been stated and agreed by the full Board.

Good practices to consider...	Things to avoid...
Make sure that the "risk appetite" statement gives the committee a solid basis for assessing risk exposures and discussing how to bring these back into line with what has been agreed. The concept of "risk appetite" can be tricky and, at times, distinctly unhelpful, especially for non-financial risks. But a board should be giving its committee and management a clear, documented steer on what is acceptable for each major risk – whether strategic, financial, operational or reputational. That doesn't mean it has to be quantified (often a fool's errand) but qualitative, directional guidance can often be enough if it is detailed.	Producing short aspirational statements of risk appetite which become meaningless when you try to make operational sense of them (with operational risks particularly prone to this). This doesn't help management, or the committee, judge how far the current risk exposure is out of line with where we want to be – or the business can support. Risk appetite statements – whether quantified or directional – work well if they are supported by good analysis, some detail and a narrative description of where the business needs to head. And often it can be best communicated by referring to decisions actually taken or case studies – rather than through conceptual statements. Too often we see boards giving up on the concept of "risk appetite" before they've really got stuck into it – often because the discussion is at too high a level, and usually too short.
Ask the "risk committee" to develop the "risk appetite" guidance before its goes to the full board meeting.	Expecting a quickish discussion in the board meeting to result in something useful. It can do – but only if the committee members have acted as "sherpas" in thinking through the objective, the detail and the way it needs to be presented.
Draw a clear distinction between board and committee discussions.	The "risk committee" discussion becoming the board discussion. Many of the same people might be in the room but (1) some directors might not be – and they need a proper opportunity to be involved (2) the chairman is a different person with a different style, perspective and (possibly) set of priorities and (3) it's a different forum with a different atmosphere and dynamics and objectives. So if it's strategic discussions around appetite and acceptability – make sure there's a proper discussion in the full board meeting, not just a quick "we've already dealt with this in the committee".

Good practices to consider...	Things to avoid...
Make sure attendance at the "risk committee" meetings is the outcome of proper consideration. For a start, the risk committee chairman needs to have a good idea of who is going to be there and why: are they literally there as "silent observers" or are they there to contribute? If so, what's their role versus the committee members'? Are they expected to prepare in the same way? If not, should this influence the way they participate? And do the benefits of full NED attendance (a shared view) outweigh the possible downsides (see opposite).	Letting attendance by non-committee member directors just come about informally – and become something which non-members slide in and out of. Yes, it might be one of the more interesting committees (although you might have to endure sitting through a lot of accounting stuff) and it's probably useful as an information source too. But the dynamics change when there are more bodies around the table – and especially when not everybody's there and attendance across meetings (or for the whole of a meeting) isn't consistent. Also, it can mean that board days become even more compressed for all the directors, with a possible impact on energy levels and attention span in other meetings. Furthermore, NED time is a scarce resource and needs to be used sparingly eg there might be less time spent on preparing for the other meetings or sitting down with management. And scheduling can become even more fraught.
Maintain a clear distinction between the role and responsibilities of committee members and of the other directors who might attend.	Allowing wider attention to dilute the sense of a committee working as just that – a small group of people with a specific, specialist focus who base their discussion on detailed preparation and recognise their particular responsibilities as a member of the committee. So when others are there, particular consideration needs to be given by the committee chairman to where the members sit and how they are included in the discussion: they need to feel like a committee, not just individuals mixed up with their other colleagues.
Be wary of detail and creep. If the information is becoming too detailed and based around risk registers with superfluous "information", make a specific request to cut it back and give clear guidance on the level of detail you want to see. Don't just assume that the CRO can guess what you are thinking.	Accepting lengthy reports with management detail which is provided to the committee "because it's available". Non-executive oversight committees don't need to know the ins and outs of the mitigation approach – and they certainly don't find it useful to be given detailed definitions of risks. Put simply, they want to know how we're exposed and what we're doing about it. (On the other hand, they're not going to be happy with glossing over along the lines of "don't worry – we're managing it".) Just because the committee asked for more detail on one thing on one occasion, that doesn't mean it must become a standard part of the report.
Ask for analysis not just data.	Accepting a report from the CRO which simply provides data and fails to set out his/her opinion on whether the risk profile, a developing trend or a particular material risk position is acceptable. Someone in that role should be providing an opinion (and a solution), not just information.

Good practices to consider...	Things to avoid...
Hold the management accountable directly rather than expecting the CRO (or other parts of the "second" or "third" lines) to speak up for them – or possibly take the criticism.	Relying too much on the CEO or the "second line". It's "first line" management's responsibility to manage the risks – so bring them into the meeting to hear first hand if it's practical rather than treating the CRO as the intermediary. If the executive directors are in the meetings they may well take responsibility – but do they have the detailed picture?
Consider the gaps in risk coverage. Regularly ask: are there areas of "big risks" that are falling outside the oversight of the "risk committee"? If so, are they being picked up elsewhere?	Losing sight of some big risks. With "cyber" being a hot topic, nowadays most "risk committees" have it firmly on the agenda. But other areas might be falling between the cracks – the integrity of non-financial information systems is a good example, the "culture/behaviour" programme another – along with "change risk". So stand back from time to time and ask: what are the significant threats to our business performance – and where is the board-level oversight sitting?"
Do some deep dives. Many committees find it helpful – possibly every meeting – to do a detailed review of a specific risk area.	Skimming over the risks at considerable height and never really getting to an adequate understanding of how we are exposed and what we are doing about it. Bring the right management in and look forward to an in-depth lesson and discussion.
Think about the impact of risk management when assessing its effectiveness: is it really making a difference to the way we work and make decisions?	Equating having good processes with effectiveness. Just because we have an ERM system that looks and feels like everybody else's doesn't mean to say that we have good risk management. The system may be "state of the art" and work as a process, but does it have much impact on what we do or the outcomes?
Include the Head of Internal Audit (HIA) in the risk committee meetings (if you have a separate risk and audit committees).	Thinking the HIA is all about the audit committee. He/she will have very good insight into the control environment and emerging threats/risks – as well as a picture of the risk culture. That's important information that needs to form part of the risk oversight discussion.
Liaise well across the board committees. That means not just the audit committee (if separate) but also the remuneration committee, to help make sure that the link between reward and risk-taking is surfaced.	Working in a committee silo. Cross-membership of committees will help but it's not always fully covering the ground. And it still needs the "cross-members" to be aware of their role as the link and to make sure there is good communication across committees (and particularly between chairmen).

Good practices to consider...	Things to avoid...
Draw on the work of the management risk committee. And make sure there's a clear understanding of the different roles of an executive committee and one that's there for independent oversight.	Failing to draw on the insight that will (or should) be available from management's discussion of risks and risk management. (And if nothing useful comes out of that, you have a different problem.) You might get what you need from the executive risk committee minutes, but having an update from the CEO or CRO in the board risk committee meeting is usually a lot better at surfacing issues.

Board agendas: are you really looking at what matters?

Independent Audit are presenting this CPD event with ICSA. An interactive and highly practical session will give delegates the opportunity to stand back and rethink their board agendas asking whether they are really helping to focus the Board on what matters.

Board Effectiveness Reviews

We are one of the UK's leading providers of board reviews, having delivered close to 250 board reviews since we were founded in 2002, including nearly half the FTSE 100. And more than 100 companies have used our online self-assessment tool, Thinking Board®.

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.

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

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

INDEPENDENT AUDIT
BOARD REVIEW