A Guide to Effective Risk Management Oversight

INDEPENDENT AUDIT

LEADERS IN BOARD EFFECTIVENESS

We often hear complaints from Non-Executive members of Audit and Risk Committees that "We're not getting what we should out of our Risk Management'." This guide is adapted from a December 2021 webinar presented by our founder and partner Richard Sheath discussing the challenges Audit or Risk Committees routinely encounter and possible solutions to overcome them.

Risk Management Effectiveness

Creating a comprehensive approach to risk management enables good decisions to be made on a day-to-day basis. We often see the Risk Committee focussing almost exclusively on the Risk Management Framework. While this is an important element, a more effective risk management model includes all five elements in the diagram below:

1. Strategic Direction

Start the process by considering how the Risk Management Framework works in the context of your organisation's strategy and what challenges and uncertainties it faces both "day to day" and longer term.

2. The Framework

With your strategic direction in place, you can then evaluate your Risk Management Framework to determine if the processes and structures fit those purposes and where you have gaps to address.

3. Behaviour and Culture

You will want to look at the effectiveness of the Risk Management Framework within the culture of your organisation. Sometimes following defined processes for Risk Management can be very effective but attitudes to risk may vary enormously depending on the context. Your framework should take this into account.

4. Management monitoring

Board committees must have good sight of how management is making decisions and assessing day-to-day risks. A good way to get assurance is to do a walk-through of key business processes, asking management how they use risk assessment in practice at each step.

5. Assessing what happened

We rarely see board committees take time to do this. It is inevitable that things go wrong, and when they do, it's important to ask what has been learned, what has changed since, and whether there are any thematic issues that should be applied across the business. This requires discussion and some detailed work, but the Committee needs to fully understand these issues and their implications for the business and how well they are being managed.

The best way to know if a system really works is to ask the people who use it. At Independent Audit we have a saying, "If it's useful it gets done". So, it's important to check that the process actually works for the people who use it.

Avoid Thinking in Silos

Risk, Compliance, IT, Internal Audit are all connected in practice, especially in relation to culture. However, they generally produce separate, unconnected reports. Risk Management Reports that combine Risk, Compliance, IT, Audit and Conduct can effectively draw out the thematic issues most relevant to the business.

Future Planning

Since the pandemic, there has been a tendency for boards to be more short-term in their thinking, which is very understandable – but this can be at the cost of much-needed longer-term thinking.

Prioritising Future Risk Discussions

Rethink how time is used in meetings and schedule regular meetings specifically for this purpose.

- Often the majority of meeting time is taken up with management presentations which often simply reiterate what has been previously shared in board papers. This time could be better spent in discussion.
- Don't wait until the annual strategy day to have these conversations. The Committee could hold an Open Thinking Session, perhaps twice a year, to think through things that might strike without warning.
- Above all, make sure you keep relating risk discussions to overall strategy.

Focusing Future Risk Discussions

We often hear that "There are too many possible risks to think through". You can apply these three steps to focus your board on what really matters.

- Ask your management team, "What are your top three concerns about what could go wrong longer term?"
- Emphasize the key obstacles and probable impact in your reporting so NEDs have a clear sense of what issues to focus on.
- And, narrow down the black swans so you have a reasonable list of the top four or five priority risk issues to address.

Maintaining a Strategic Direction

Principal risks should ideally generate a discussion on strategic direction. However, all too often, we witness risk committee discussions that are squarely focused on the Annual Report entry. Principal risks should be discussed all the time, not just before the Annual Report is due:

- Make the concept of risk appetite relevant to your business.
- Work out what you want from the principal risk discussion.
- Make risk integral across the agenda so that it becomes something valuable rather than just a requirement that needs to be covered.

"What are your top three concerns about what could go wrong longer term?"

Responding To ESG

The challenge with responding to the ESG imperative is that there is no one right approach.

Define What ESG Means for your Organisation

ESG actually brings together three separate concepts that are quite different, with varying strategic implications. It is important to first work out what each part means for your organisation. Often we observe discussions that include only one aspect, such as Health and Safety, or the Environment, but label them as ESG. We recommend that our clients get very clear on what ESG means to their strategy and business priorities and use specific language to communicate those priorities.

What is the new risk universe as ESG drives change?

Organisational culture	Risk culture	Investor relations
Branding	Communications	Capital investment
Product/service design	Controls	Assurance
Risk management	Welfare	Communities
Health & safety	Recruitment & retention	Reporting
Reward & motivation	Financial investments	Fair treatment
Diversity & inclusion	Contractors	Procurement
Suppliers	Purpose & values	

- The Risk Committee needs to think through the control implications for every area, ensuring they have a handle on the whole picture and know where the priorities lie.
- ESG Priorities have an impact on culture and the new mindset everyone in the organisation will need to adopt in making decisions and dealing with internal and external stakeholders. So, the Committee needs to get a picture of how culture is changing within the organisation.
- When scenario planning, it helps to think of each of the different elements within the context of what is most important to your customers to prioritise areas for focus and tease out potential impact in each area.

Future Risk Assessment

The risk universe is changing. Expectations of organisations are growing, so oversight needs to keep pace. Now is the time to develop a “Principal Risk List for the Future” which is driven by ESG priorities, and the board and its committees need to keep the subject front and centre.

Risk Reporting

Ultimately, the Committee needs to receive a clear and actionable report. Here are some practical suggestions for improving reports to ensure that the most important information is clearly communicated in a way that is actionable for the Committee.

Presentation Matters

It may sound superficial, but we often hear NEDs complain about fonts which are too small to be read on a screen. Consequently, they struggle to see the detail in tables and data.

If you are a CRO preparing papers to present to the relevant board committee:

- Make sure the font is legible as it appears on screen.
- Cut out unnecessary detail and highlight what matters most.
- Don't leave it to NEDs to work out what they should focus on. Make it your job to show them what is priority.

Provide Context & Focus

The introduction/summary page of the risk report isn't always as helpful as it might be. To improve its value, consider the following:

- NEDs want to know what has changed and why, so make sure you explain this clearly as well as stating the resulting implications.
- Focus on the Top 5 priorities for consideration.
- Consider your use of heat maps carefully. Often, we see board committees focus heavily on the highest scores. But, it's important to think through what will surface the risk matters which the Board really needs to focus on.
- Probability and Impact are both judgements that are hard to quantify. Many risks don't lend themselves to quantifiable calculation, so you need to find other ways to address them.
- When there is a significant shift from gross to net risk (post mitigation), make sure there is a full explanation and/or discussion of the reasons.

Priorities for Action

- Often the CRO report doesn't include their opinion. However, the Board really needs to know what the CRO sees as the main things the organisation should be focusing on. Hearing their opinion only in the verbal presentation doesn't allow NEDs time to think things through before the meeting. So, make sure the first section of the CRO report contains an upfront opinion/analytical section that tells the Committee what they see as the priorities.
- Rather than relying purely on analysis, the Risk/Audit Committee should also be pushing First Line risk owners (the managers responsible for specific business areas) to raise their concerns. So be sure to include them. Bring them forward for the Board.
- It's important to ask, "Why does this matter?" Often risk oversight discussions are purely procedural, focusing on the risk register and principal risk list rather than considering what the risk implications are for the strategy, achieving budget goals, share value and so on. Risk reporting should always communicate this relevance.

To watch or listen to the complete presentation, you can download the webinar recording **here.**

For more information, contact:

Remneek Sangar, Client Relationship Director | **+44 (0)7549 032722** | **remneek.sangar@independentaudit.com**

INDEPENDENT AUDIT

LEADERS IN BOARD EFFECTIVENESS