Why you might want a pilot running your Risk Committee

There's a saying in aviation: 'Never fly in the same cockpit with someone braver than you'. Risk management for a pilot is literally a matter of life and death. Have you ever asked yourself whether you would share a boardroom table with executives braver than you are?

Company risks are often presented as long shopping lists; each with a reassuring comment, about how it's unlikely but that it's covered off. A typical audit committee, and now the whole board, will be faced by this list and asked to opine as to whether this is a fair summary of the risks facing the business and the mitigations. The board, or more likely the CFO, will then select a dozen of the juicier risks to list in the annual report.

Neither the non-executive director nor the annual report reader is likely ever to gain much nourishment from this exercise. However, the drive of the regulators to be seen to get action from board on risk will be satiated for another year. Has this sort of exercise ever helped to prevent a financial failure?

It's not a surprise to find that aviation has developed a more insightful way of looking at risk. As the great aviator Ernest K. Gann wrote; "Rule books are paper - they will not cushion a sudden meeting of stone and metal." The director could well substitute Annual Report for rule book.

Aviation has developed a Threat and Error Management model, which includes looking at risks by their type and then applying a three stage management process; avoid, trap and mitigate, which can equally be applied to business risks.

1. Categorising the types of risks

There are three high level categories of risks and events; unexpected external, expected external, and internal risks. We are, of course, here in the realms of Rumsfeld's known unknowns and unknown unknowns. Rumsfeld incidentally was a naval pilot himself. An event is when a risk actually becomes a reality.

- Unexpected external risks are, by definition, the most difficult to foresee. To quote Gann again, "The emergencies you train for almost never happen. It's the one you can't train for that kills you." It was, for example, the failure of confidence in AAA securities that was one of the key problems causing the recent financial crisis, yet almost no one predicted this risk could happen.

- An expected external risk might be a rise in inflation or interest rates. These are risks that might reasonable be expected to have a chance of happening. They are the most common type to appear on a risk register, as they are easy to imagine and therefore easier to plan for.

- Internal risks are those that are under your control in the business and are the ones most looked at in traditional control systems. These tend not to be so prominent in external communication of a business's risk, as to acknowledge them implies that the control systems are not fully reliable.

2. 'Threat and error management'

Avoid

Clearly the best outcome is to avoid a risk becoming an event. To achieve this, companies put processes and controls in place or take pre-emptive avoiding action. This is generally applicable only to expected external risks, as it is a tough task to avoid an unexpected external risk. Some expected external risks are also not avoidable. For example, a rise in general interest rates is not within a company's control, but a campaign against, say working practices, could be avoided by pre-emptively maintaining high standards of care for employees.

Most internal risks are avoided by careful management, strong defined processes and robust control systems. For example, fraud can be deterred by visible deterrents and controls. Increasing visibility of such deterrents (eg cameras) is in fact a prime avoidance technique. However, in any company, internal risks will crystallise into events.

Trap

No matter how good the controls and avoidance techniques are, the assumption should be that there will be a breach. All humans make mistakes. No avoidance system is ever 100% full proof. The next stage is therefore to try to trap the event. This is where information systems are crucial.

It is essential to know that the first defence (avoidance) has been breached, so there has to be an alert. Directors need to understand what systems there are to alert managers to any possible, upcoming or actual breaches.

When an event happens, management needs to (a) notice it and (b) interpret it as important. An unexpected external event is particularly tricky to pick up every time. It does not fit easily into a standard control system, as it may not even be monitored. The event may however cause a performance measure or a forecast to move, which may then trigger an alert.

Generally you hope that senior management has the 'helicopter vision' to spot unexpected strategic events, but at working level, it may be any employee who spots an unexpected new risk; for example a sudden bout of arson in a local community. The person who initially notices the event may well not be the same as the one who spots its significance.

How good are the communication systems so that these different people can be linked together? The simplest example here would be an employee looking at a bank statement, and querying a suspect transaction. In this case there should be a system to flag and investigate unusual transaction, and an agreed procedure that follows. However, the information system on other less structured risks may be an informal network; for example a casual mention of something new to someone else over the coffee machine. It is easy to forget the informal information systems, but these can be very important.

In summary, the important features of trapping are; noticing an event and then interpreting it as important. The methods for achieving this are both formal and

informal information systems. This may also require preliminary investigation to understand the nature of the event, including cause, extent and implications. Trapping unexpected external events is particularly problematic, as, by definition, you do not know what you are looking for.

Mitigate

Having trapped the event, the task is now to mitigate its effects. This may well require in-depth investigation, in order to understand fully what happened, which controls failed and what can be done to minimise the ill effects of the breach.

The direct and indirect effects of the breach need to be identified. Indirect effects can be often missed. The event itself may be mitigated by, for example, removing an errant individual, but there may be a loss of confidence in the that department that causes others to move work elsewhere or put in their own informal double checks, reducing efficiency.

The business may need to compensate and replan for the event. A rise in interest rates, for example, may cause the business to reduce costs elsewhere or conserve cash. A spate of arson is likely to cause the business to both review its insurance cover and improve fire suppressant systems.

Finally the business needs to learn from the breach to reframe processes and controls. In rare cases, it may decide that nothing could be done, particularly from unexpected external events. However generally there will be lessons and enhanced procedures that will either reduce the chances of a future breach, or will mitigate its effects. This tends to be, at least on internal risks, the province of the internal audit recommendations. This feedback is often the most important part of the response, as the company has learnt how better to handle the risk and to prevent future such events.

Summary – a risk management framework.

Avoid	Trap	Mitigate
Visible deterrence	Information systems	In-depth investigation
Defined processes and robust control systems	Informal and formal communication	Direct and indirect effects identified
	Interpretation and sensitivity	Event compensation
	Preliminary investigation	Business replanning
		Feedback: reframe processes and controls

Applying this thorough framework could help companies and boards better understand and manage all aspects of risks. In particular, it focuses on the importance of; informal and formal communication, the role of everyone in the business to spot possible events, timely and comprehensive information systems, compensation, and feedback.

It also emphasises that every risk should be assumed to be going to become an event. This forces proper consideration of trapping and mitigating, which otherwise tend to be assumed not to need detailed thought. It's likely, as Gann said, that it will be the risks that you never thought of, or never believed could happen, that will be the most painful. Just ask the people who used to believe in AAA bonds.

Simon Laffin

www.simonlaffin.com