Think like a pilot:
How a non-executive director can challenge business risks.

Have you, as a non-executive, ever sat there wondering how you can realistically review the long shopping list of corporate risks? What value can you add? How can you systematically challenge them? And when something goes wrong, the executives explain what happened, but how does a non-executive go deeper to understand if there are systematic issues, rather than one-off bad luck?

These are real questions that non-executives face all the time. There are however pointers from aviation, an industry that really understands risk management. In an earlier article I reviewed how aviation categorises and reviews risks, by sub-dividing them into expected external, unexpected external and internal risks.

For most non-executives, internal risks are the most commonly discussed ones, as they are, or should be, under the control of the business. Aviation has three levels of risk management; avoid, trap, mitigate.

Avoid

Any organisation should have basic defences to avoid risks becoming events. The major defences are the control environment, systems and procedures. The control environment comprises culture and controls. Is the atmosphere lax or do people expect things to be done by the book? Are short-cuts or compromises allowed? Are whistle-blowers encouraged? Procedures include policies, methodologies and rules. Who can authorise what, and how does an action get approved? Systems should follow from the procedures (and not the other way round), as rules and methodologies are coded into systems to automate processes.

Defences can be overt or covert. Strong password disciplines on systems, for example, are not only a control, but also a visible deterrent, dissuading some people from trying to break into the systems. The first line of any defence is always deterrence. So a strong control environment must first be understood and acknowledged to be so. There may even be a value in bluffing, giving the impression that controls are even stronger than they are. The classic example of this is dummy cameras. Another is supermarkets that encourage local police to use their staff canteens. The sight of uniformed officers walking through the store always has a highly salutary effect on shoplifters.

Trap

A control has failed, and an internal risk has become an event. This now should be understood as either a process failure or a violation.

a. Process failures

These are unintentional control errors, for example, an invoice that gets paid twice because a clerk or a system fails to stop a duplicate. You can normally divide these into skill-based and knowledge-based;

1. **Skill-based** errors are often failures arising from human frailties, such as forgetting to check something, or even a physical slip or fall. They are a result of an operator being human. Every person makes mistakes, and so control systems have to be resilient to human error. A slip occurs when a person intends to do something, but inadvertently does something else, for example, pressing the wrong button or dialling the wrong number. A lapse occurs when someone forgets to do something. For example, an employee forgets to log off a computer or fails to check a security system.

2. **Knowledge-based** failures arise from someone's lack of expertise or information. A buyer who is new to the job might not know that they need to check a new supplier is already on an approved list, or has certified that they apply certain ethical standards. A manager may simply not know how to deal with a situation. A person lacking the right skills is a knowledge failure, not a skill one.

b. Violations:

These are deliberate breaches of controls and processes. They can be either routine or exceptional.

1. Routine breaches are fairly common ones. It may be 'accepted' practice for employees to share a login code, possibly even one written on a post-it note on a terminal. Procedures may be too cumbersome or out-dated to be practical, and people get used to skimping on them. So routine breaches need to be reviewed to see if the problem is with the process, rather than the violators. The violators might be keeping a process going that otherwise simply would not work.

Routine breaches are most likely to be failures of the avoidance system, instigated neither out of malice nor incompetence, but by humans reacting to a control system that hinders what they perceive as their everyday roles.

2. Exceptional breaches come in many different guises. They may result from exceptional situations that were not envisaged in the standard process. An unexpected external event may have happened and the staff on the spot then had to make a quick decision about how to react, without the time to consult a manual or a superior. By contrast, a violation may even occur out of boredom. The Chernobyl reactor fire started as a result of unauthorised experiments by bored staff. Corruption or criminal behaviour might cause an employee to deliberately violate procedures. Finally, a disaffected employee could violate in order to sabotage a process or company.

Exceptional breaches are more likely to represent a serious failure of the control system to envisage certain events or a person intent on abusing the system.

Mitigate

The difference between knowledge and skill failures is important.

- **A skill-based error** may reflect the need to change the ergonomics (for example, if two options on a system are similar, eventually someone will click the wrong one or the same with two very similar levers on a

machine), or the need to ensure people are careful when long-standing processes are changes (as the operator is very likely to revert unintentionally to their previously learned behaviour). Skill-based errors should be easier to trap, as they may be predictable. For example, most computer input systems put extensive effort into trapping obvious mistakes. Google, for instance, will try to spot a spelling mistake in a query, and offer a "Did you mean?" alternative.

It is important to distinguish everyday slips from outright carelessness. The mitigation for the latter might be punishing an individual, but, for the former, it is a process solution, making it more difficult to commit common slips and providing better immediate trapping of when they do occur.

- **Knowledge-based errors** generally represent a failure to provide training. The knowledge usually exists, but hasn't been disseminated to the right people. The mitigation may be to review training standards and provide remedial education.

- **Routine violations** are likely to require a change in the process or system to make it less attractive to violate than to comply with controls. It may be of course that sanctions also need to be taken against the violators if their actions are unreasonable.

- **Exceptional violations** are more difficult to generalise. Ensuring that risk management has encompassed less likely scenarios will help, as will cultural measures that reduce boredom and identify employee disaffection.

Conclusion

Non-executive directors need to challenge risks more, but they often don't know how to. This classification can help to challenge executives about risks and events. It moves beyond knee-jerk reactions to errors, failures and violations, which often focus on condemnation of individual behaviour. It accepts human frailty, and points towards making system and processes resilient to operator error. It forces managers to distinguish control breaches, which serve to keep the organisation running, from malevolent violations that undermine controls.

Next time you fly, take comfort from the risk management that has made commercial aviation such a safe form of travel. Then get back to the office, and use it in your boardroom.