



Governance, Risk Management, Compliance and Ethics

Fast Assist for Main Board Directors

1. **Governance** is about knowing the long term plan, asking the big and basic questions and; intelligently interrogating the answers. .
2. **Risk management** is about common sense. It is about safe passage through otherwise uncertain terrain.
3. **Compliance** is an operational imperative. It is a regulatory requirement and a sunken cost. It doesn't always add value¹.
4. **Ethics** is overarching. It is about doing the right thing, particularly when in doubt
5. **A practical view of risk;** It is useful to think in terms of practical obstacles to business objectives. Think of what can stop, delay, and obstruct successful execution of objectives. When you think in terms of obstacles to successful execution of objectives (strategic, financial, operational, hazard) you arm yourself with knowledge of what questions to ask. Don't stop asking questions until you have uncovered the big and basic facts. Don't get distracted by risk management and compliance jargon.
6. Companies are required to take risks and to have **safety nets** when doing so.

A profile of identified risks and mitigation measures is called a **risk register**. As Directors, we should be concerned that many risk registers do not contain the things which really worry people, the things which are too heavy to be put on paper; the things which are whispered about but not committed to paper. As Directors, we need to be sure that there are no gaps. Gaps appear when:

- a. Taking **strategic steps**² into unknown territory,
- b. Making **cutbacks** that may lead to shortcuts; and to mistakes

2. It is really important to understand that:

- a. The Board balances strategy with the prospect of gain. Changes in strategy precipitate changes in exposure to risk.
- b. Management is charged with the execution of an agreed plan and the tactical management of risk,
- c. Pace of change and complexity have inflationary effects on risk,
- d. Good management in our uncertain world requires an absolute resolve to achieve and maintain sustainability. **Sustainability requires resilience.** Resilience is tested against abnormal and adverse shocks and surprises. Shocks and surprises which are not abnormal and adverse are just incidents which have an operational impact but do not threaten reputation and the balance sheet. **The Board, and not management, sets scenarios for resilience testing.**

3. We can insure against risks but have to manage uncertainties. You can test this:

¹ Witness recent major corporate collapses; practically all of them attested to full compliance before collapse occurred. Their understanding of governance and risk was a fig leaf to their overall exposure to foreseeable and foreseen events.

² Over 90% of major corporate collapses are due to strategic mis-steps and operational failures (Booz, Mercer)...*witness the global financial crisis.*



- a. Ask your insurance broker, and an alternate broker, to report on your level of insurance covers over your top 10 risks. Typically 10-15% of your total risks are insurable; very often a lesser percentage is adequately covered!
- b. Ask your insurance broker, and an alternate broker, to report on the adequacy of Directors and Officers insurance cover relative to your own personal exposures. Ask about your personal exposure even after you resign as a director!

4. Questions for you to ask of management:

- a. Given the complexity³ of our operations how do we:
 - i. Ensure that we are not mixing up different categories of risk?
 - ii. Ensure that information used for input into our risk management model(s) is relevant and correct?
- b. Given complexity, and organic and acquisitive growth, do we have a common risk language across all of our operations? Where does this come from?
- c. Given complexity, and organic and acquisitive growth, do we have a common format /framework for capture of key risk based information across all of our international operations? Where does it come from?
- d. Given pace of change how do we ensure that our information is up to date?
- e. Given pace of change, and complexity, how much experience do we have of tracking events in areas of activity we were not engaged in say 3+/- years ago?
- f. Given pace of change, and complexity, how do we account for events which are very low frequency in their occurrence, but potentially lethal in their impact?
- g. If we say that an event has a one in 25, 50 etc. year chance of happening; How do we know this for sure? Is it guesswork? When did the clock start?
- h. Given all of the above, what degree of error is assumed in the risk management model(s) we are using?
- i. When degrees of error are exceeded and red flags are raised how long does it take for this information to get reported to the board? Is the information dispatched in an edited or un-edited format? If edited, who is the editor?

RMI provides a service which addresses all of the above questions in a more effective and cost efficient manner than most organisations are themselves capable of doing.

³ Complexity Issues:

- 1. Increased complexity of organisations compared to say 10 years ago,
- 2. Growing complexity of supply chain(s) / third party / counterparty relationships,
- 3. Growing complexities of the world in which we live given multiple interconnections and interdependencies,
- 4. The low to no visibility of third party vulnerabilities...legal contracts do give recourse through the courts but are of little real value when struggling to regain market share in the aftermath of a serious event,