RISK DOCTOR BRIEFING

RISK MANAGEMENT PRINCIPLES
PART 2: OGC M_o_R

© August 2011, Dr David Hillson ***FIRM, HonFAPM, PMI Fellow***

david@risk-doctor.com

The last Risk Doctor Briefing looked at eleven principles for risk management which are contained in the international risk standard ISO 31000:2009. We suggested that adopting and implementing these principles could lead to a more effective approach to managing risk. But ISO 31000:2009 is not the only risk standard that offers a set of risk principles. The UK Office of Government Commerce (OGC) is responsible for the *Management of Risk* methodology (M_o_R *) which is widely used in government and elsewhere, and the most recent M_o_R guidelines include a set of eight risk principles that can be applied in any setting or type of organisation.

The OGC M_o_R risk principles are informed by the content of ISO 31000:2009 as well as by current corporate governance guidance, so they are meant to have very broad applicability. These are the M_o_R principles:

1. *Risk management aligns continually with organisational objectives.* Risk is "uncertainty that matters", and it only matters if it could affect achievement of the objectives of the organisation. We need to understand our objectives, define how much risk is acceptable, and decide how to manage risk within those limits. When objectives or risk tolerances change, the risk process must change too.
2. *Risk management is designed to fit the current context.* Organisations operate in an external context (markets, competition, regulation etc.) as well as an internal context (culture, people and processes). Risk management must recognise and respond to the context, and change when it changes.
3. *Risk management engages stakeholders and deals with differing perceptions of risk.* Different stakeholders see risk differently, and the risk approach must take account of these perceptions. We need to recognise and counter bias, and manage stakeholder expectations regarding risk.
4. *Risk management provides clear and coherent guidance to stakeholders.* Clarity means that everyone knows what the risks are and how they are being addressed. Coherence occurs when risk is managed consistently across all levels of the organisation, and when it is communicated properly across organisational boundaries.
5. *Risk management is linked to and informs decision-making across the organisation.* We have to make decisions with incomplete or imperfect information, which makes decisions risky. The best decisions are made when we understand the risks that are associated with different options.
6. *Risk management uses historical data and facilitates learning and continual improvement.* We can improve the way we manage risk by identifying generic sources of risk and developing effective generic responses. The aim is to become more mature in our risk culture and practice.
7. *Risk management creates a culture that recognises uncertainty and supports considered risk-taking.* Every significant activity involves uncertainty and requires us to take risk. But we need to take the right level of risk, balancing risk-taking with reward. This requires a risk-mature culture that rewards proactive risk management.
8. *Risk management enables achievement of measurable organisational value.* The risk process should result in fewer threats turning into real problems. It should also help us to turn more opportunities into real benefits. Both of these will create measurable value for the organisation.

These risk principles are different from the ones suggested by ISO 31000:2009, although there is some overlap. But like ISO 31000:2009, the OGC M_o_R principles provide a framework to challenge the way we manage risk. Whichever guidance we adopt, we should think about how we are currently managing risk, and consider how these principles can help us do better.

[* Reference: UK Office of Government Commerce (OGC). 2010. *Management of Risk: Guidance for Practitioners* (third edition). London, UK: The Stationery Office. ISBN 978-0-11-331274-0]