



RISK DOCTOR BRIEFING

RISK MANAGEMENT PRINCIPLES PART 1: ISO 31000:2009



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

david@risk-doctor.com

Too many organisations use a risk process without understanding the principles that underlie effective risk management. But what are those principles? One place we might look for guidance is the international risk standard ISO 31000:2009 *Risk Management – Principles and Guidelines*, which includes a set of principles for us to consider. Each of these principles tells us something important about risk management, and together they set a challenging target for organisations who want to manage risk well.

Eleven risk principles are outlined in ISO 31000:2009. Some of them are obvious, but others may need a little explanation. These are the principles:

1. *Risk management creates and protects value.* Value is created when we achieve our objectives, and risk management helps us to optimise our performance. It also protects value by minimising the effect of downside risk, avoiding waste and rework.
2. *Risk management is an integral part of all organisational processes.* Risk management is not a stand-alone activity, and it should be “built-in not bolt-on”. Everything we do should take account of risk.
3. *Risk management is part of decision-making.* When we are faced with important situations that involve significant uncertainty, our decisions need to be risk-informed.
4. *Risk management explicitly addresses uncertainty.* All sources and forms of uncertainty need to be considered, not just “risk events”. This includes ambiguity, variability, complexity, change etc.
5. *Risk management is systematic, structured and timely.* The risk process should be conducted in a disciplined way to maximise its effectiveness and efficiency.
6. *Risk management is based on the best available information.* We will never have perfect information, but we should always be sure to use every source, being aware of its limitations.
7. *Risk management is tailored.* There is no “one-size-fits-all” approach that suits everyone. We need to adjust the process to match the specific risk challenge that we face.
8. *Risk management takes human and cultural factors into account.* Risk is managed by people not processes or techniques. We need to recognise the existence of different risk perceptions and risk attitudes.
9. *Risk management is transparent and inclusive.* We must communicate honestly about risk to our stakeholders and decision-makers, even if the message is unwelcome to some.
10. *Risk management is dynamic, iterative and responsive to change.* Risk changes constantly, and the risk process needs to stay up to date, reviewing existing risks and identifying new ones.
11. *Risk management facilitates continual improvement of the organisation.* Our management of risk should improve with time as we learn lessons from the past in order to benefit the future.

Each of these principles can make our risk management better and more effective, if we translate them into the way we actually do things in practice. If we are satisfied with the way risk management is currently working in our organisations, then perhaps we can ignore these principles. But if we want to improve our performance in this important area, the ISO 31000:2009 principles offer a good place to start.

[Other risk standards also include risk principles that aim to strengthen the way we manage risk. The next Risk Doctor Briefing will look at another set of principles contained in the *Management of Risk* (M_o_R) guidelines from the UK Office of Government Commerce.]