



September 2005

The beginning of the end for risk management?

Has risk management been over-hyped and is it due for a backlash? This question has enormous significance for national security as risk management is the basis for the nation's response to the threat of terrorism. (See *Panel 1: Risk management at the centre of national security*)

All management techniques during their lifecycle will hit a peak of interest before declining rapidly. This occurred with management by objectives, benchmarking and quality management. And it will occur with risk management – it's just a question of when.

Considering this issue in such a blunt way should not be misconstrued as questioning risk management's validity. Risk management can deliver enormous benefits in certain situations, but will not live up to expectations when applied inappropriately. One only has to review recent investigative reports of government programs to see the frequency with which problems with the implementation of risk management processes are identified.

The best way to determine where risk management lies on its lifecycle curve is to compare it with the fate of quality management. Quality management offers an ideal comparison because of its similarities with risk management.

Both started out as technical disciplines focused on operational effectiveness – quality control in manufacturing and risk identification in insurance and safety. Both morphed into generalised

management philosophies encompassing the entire organisation – quality becoming Total Quality Management (TQM) and risk became Enterprise Risk Management. Both had undisputed success in technical areas like statistical quality control or project risk assessment but both lacked solid cost-benefit evidence to prove their effectiveness at an organisation level.

Both seem to follow the typical five stage lifecycle for management techniques. See *Panel 2- The lifecycle of quality and risk management*.

The apex of success for quality management was about 15 years ago. This was when it had become a worldwide phenomenon. The Australian Organisation for Quality chapters boasted thousands of members,

Panel 1: Risk management at the centre of national security

The importance of risk management for the nation's national security posture is reflected in its centrality in various government strategic documents.

For example, the publication—*Protecting Australia Against Terrorism*—which sets out the elements of Australia's national counter-terrorism policy and arrangements, states that one of five key principles underpinning the government's counter-terrorism planning is "sound risk management approaches that deliver the maximum level of security while making best use of the resources available to us".

The *Critical Infrastructure Protection National Strategy* which sets out an overarching statement of principles for critical infrastructure protection in Australia, states that "by applying risk management techniques, attention can be focused on areas of greatest risk, taking into account the threat, relative criticality, the existing level of protective security and the effectiveness of available mitigation strategies for business".

National Security Practice Notes is a publication series that covers topical issues which are of critical importance to building national and domestic security capability. They are aimed at practitioners in the intelligence, security, law enforcement, emergency services and related national security areas.

The Australian Homeland Security Research Centre undertakes independent, evidence-based analysis of domestic security issues.



National Security Practice is a publication series that covers topical issues which are of critical importance to building national and domestic security capability.

National Security Practice is part of the research program of the Australian Homeland Security Research Centre.
Australian Homeland Security Research Centre
Tel 02 6161 5143, Fax 02 6161 5144
PO Box 295, Curtin ACT 2605
info@HomelandSecurity.org.au
www.HomelandSecurity.org.au
Copyright 2005. All rights reserved.

hundreds of Australian organisations had their management systems certified to ISO quality standards, and hundreds of articles appeared every year praising TQM. Today little is heard of quality management, and when it is mentioned in the mainstream media it is often as the butt of Dilbertesque jokes.

Identifying the current position of risk management along its lifecycle is difficult without the benefit of hindsight.¹ However, the frequency which it is mentioned in the media provides an indication. This places its creation phase in the late 1990s with the evolution phase around the early 2000s. The evolution phase was relatively short as the shocks of global terrorism and other uncertainties all required immediate action which meant that the case for change did not have to be argued.

It appears we are now in the time lag phase where the technique is being implemented throughout Australian governments and businesses. Its penetration is no better illustrated than in the central role it plays in the Australian Government's strategy for national security. Risk management features as one of just four key principles in the strategy. It states that "sound risk management will deliver the maximum level of security while making best use of the resources available". Its dominance in the corporate world is also apparent for risk has become the filter through which all board and senior management decisions pass, at least at a rhetorical level.

The similarity between quality management and risk management also provides an indication of the problems that will lead to dissatisfaction with risk. These include that in many of the organisations in

which it is implemented:

- It is inordinately resource intensive. This is not only during the risk identification period but also in the ongoing maintenance of risk registers and implementation of risk treatments.
- It is too heavily focused on documentation which is driven by (misunderstood) auditing requirements.
- It provides little usable information at the corporate governance level.²

Risk management also faces several other significant problems which are contributing to scepticism towards its universality. For example, the majority of its focus is on preventing an unwanted event from occurring such as toxic gas leaks. Little corresponding effort is given to exploiting upside risks such as capturing new market opportunities. Another example is that the risk formula of likelihood and consequences does not allow for the easy comparison with non-probabilistic risks such as terrorist attacks.

Conclusion

While it is too early to claim that the honeymoon with risk management is over, its universal acclaim is bound to decline over the next few years as we move into the scepticism phase of its lifecycle.

What this means for those involved in risk management is that they need to be sensitive to the signs of a shift in acceptability for the tool. What needs to be looked for is the tipping point which marks the point at which risk management goes from *de rigueur* to *passé*.

This point may be easy to spot, for example when a review of a major failure finds that risk management arrangements were a root cause of the problem. However, the point may be much harder to identify as the cause is an accumulation of discontentment which builds up glacially slowly and mostly unnoticed until suddenly faith in risk management collapses. Another sign of an impending change is increasing emphasis on undertaking activities because it is prudent rather than because of an identified threat, and spending more on designing out risks rather than relying on the more cost effective operational security activities, because of a loss of faith in the latter's ongoing effectiveness.

A future National Security Practice Note will look at the systems that could be put in place in anticipation of a decline in support for the then current form of risk management practice.

Panel 2- The lifecycle of quality and risk management

Most management techniques follow a five stage lifecycle.

The first phase is creation. This is where a crisis is claimed and a solution identified which offers to bring organisations away from the brink. The crisis which boosted quality from a practice backwater to international prominence was the lack of competitiveness of US manufacturing. The quality solution was claimed to be able to reshape an organisation, making it customer focused while lowering costs. The crisis which underpinned the popularity of risk management was massive uncertainty caused by globalisation, the tech-wreck of the late 1990s, the September 11 2001 attacks, SARS and corporate malfeasance. The risk solution was claimed to fundamentally change the way challenges were dealt with by an organisation, offering more certainty and continuity.

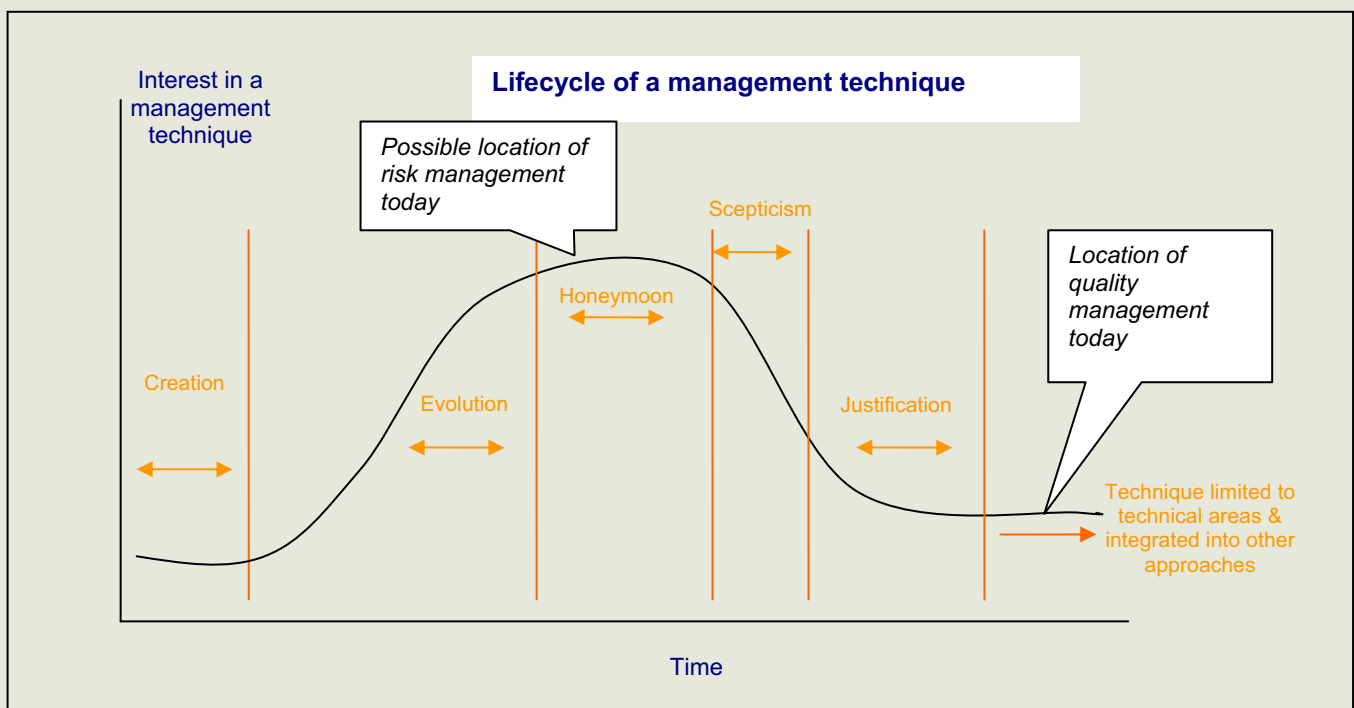
The second phase is evolution. This is where numerous stories about the technique's success are promulgated. Invariably these stories have the following components. The technique is universally applicable, it should not be seen as a quick fix, it requires substantial management support, and it is based on rational decision making emphasising goals and causality. During the evolution phase, the promotion of the technique becomes increasingly evangelistic and penetrates the mainstream media. Catchy and simplistic rhetoric dominates, such as 'quality is free' or 'risk optimisation not minimisation'.

The third phase is the honeymoon period. This is the honeymoon period in which the new technique becomes widely implemented before user reaction and measurable outcomes appear. It is also the time in which standards for the technique are formalised - the ISO 9000 series for quality and AS/NZS 4360 for risk. Interestingly, these standards are performance based and deliberately avoid a prescriptive approach. However, users invariably demand much more explicit guidance on implementation, leading to the popularity of tools which allow people to follow a formulaic approach, based on ticking boxes.

The fourth phase is scepticism. At the beginning of this phase, revisionist tales appear about the limitations of the approach, warning that it has become a management fad. By the phase's end, detailed accounts appear, proving that the technique has not lived up to expectations.

The final phase is justification. This period is when the initiative's champions, who are witnessing its demise, protect their status by attributing the blame for its failure. Responsibility is commonly laid at the feet of management for its lack of leadership, or inappropriate implementation. Other commonly claimed causes are a lack of resources, insufficient time, and recalcitrant staff.

Just as each technique had a life before it was 'discovered', it will continue to have one after it has lost its mass appeal. Invariably, it will return to its technical base as well as being absorbed into other approaches.



Panel 3 - Potential problems with risk management

Almost every report on major incidents contains some commentary on risk management failures. Examples are the *Palmer Inquiry into Cornelia Rau Matter*, the *Report of the Inquiry into the Australian Intelligence Agencies*, and ANAO's *Protecting Australian Missions and Staff Overseas*.

Below is a list of common problems with risk management.

- **As managing risks is an exercise in professional opinion, the judgements may be incorrect.** The three main reasons for incorrect judgements are:
 - **Lack of skill.** Risk management requires subject matter expertise, experience in the risk management process and other skills. A lack of any of these can undermine the risk management outputs by confusing problems with risks, not correctly identifying relevant risks or even failing to manage risks.
 - **Lack of information required to identify, analyse and evaluate risks.** Risk management is predicated on having relevant information, whether it is objective or subjective, certain or uncertain. Without relevant information, it can result in fundamental mis-assessment such as likelihoods being wrongly identified, impact categories being determined as linear when they are not, or even risks being treated as independent when in fact they are dependant. Knowing when all the relevant information is available can be extremely difficult in highly complex systems such as land transport.³
 - **Bias.** Risk management requires that analysts be sensitive to different risk perceptions rather than internalising them as bias. By being overly sensitive or second-guessing certain risk perspectives, such as political risk, the risk management outcomes may not be optimal. Other bias can occur due to selective attention to certain kinds of hazards and giving undue influence to the most vocal interest groups. This is because risk perceptions are influenced by the 'point of reference' of the assessor.
- **A focus on elements within a system may overlook systemic risks.** There is a natural tendency to break down a system into elements of a manageable size. This tendency is reinforced when the system contains some elements that are within one organisation's control and the rest outside it. Consequently, an organisation will inevitably focus more on the elements that are under its direct control and focus less on areas where it has less control. This can lead to risk treatments that are optimal from an element perspective, but have little impact on systemic weaknesses. As systemic weaknesses are often not in any one organisation's control, these issues can often be ignored. Factors preventing a holistic view being taken include organisational priorities and responsibilities, jurisdictional specialisations, and a lack of system understanding, and a reliance on software tools without a feel for the accuracy of their outputs.
- **The context statement may be inadequate.** Risk management is dependant on having a sound context, as it defines the environment, the stakeholders, the risk criteria, level of acceptable risks, resource availability and the cost of doing nothing, amongst other factors.
- **While a mitigation action may result in a reduction in target risks, it may at the same time increase countervailing risks.** For example, increasing access control will reduce the risk of criminals entering a building but it may increase the risk of staff being trapped in the building if a fire occurs.
- **There is a natural reluctance by organisations to document all their risks as others can use it against them.** For example, terrorists could use the information for physical destruction, corporate competitors could use the information for commercial destruction by highlighting weaknesses to gain market share, and governments could use the information for political advantage by shifting blame in the event of an incident.
- **Organisations may have a culture that does not deal constructively with negative information.** Risks are about negative events (failures or losses). Many organisational cultures attempt to be optimistic, and tag pessimistic assessments as "not in line with corporate values". This can inhibit the identification and mitigation of risks, and result in the risk managers' task being perceived as a necessary evil, which is tolerated but not supported.

Footnotes

1 However some would contend that by using the Capability Maturity Model Integration (CMMI), the position of the Australian Government is about level 2 of the 5 levels.
 2 The Australian Stock Exchange Corporate Governance Guidelines provide an

example of how risk management information can provide valuable information that informs the company board.
 3 Qualitative and semi-quantitative risk management is at best a 'best guess'. The 'best guess' will always be limited by the quality and completeness of available information.

Security Jobs Central

Positions for security, risk and intelligence professionals



Sign up for your free weekly email listing positions vacant at
www.securityjobscentral.com.au