RISK MANAGEMENT AND PERFORMANCE MANAGEMENT

Introduction

The purpose of this paper is to discuss some similarities and contrasts between risk management and performance management. Such comparison can throw light on both disciplines.

The conventional meaning of risk indicates issues or factors to avoid. Performance management (which in this context means identifying performance indicators and then managing to achieve success as defined by those indicators) is based on setting targets to achieve. These may be considered as two faces of the same coin. They are both concerned with management principles designed to assess and then improve performance.

Within the Evaluation community, it is likely that readers are more familiar with performance measures, for example the program logic formulation, than they will be with risk management. Therefore, some initial observations are made about risk management before comparing and contrasting the two approaches.

Risk Management

In recent times, many organisations have adopted risk management as a key element of management. The adoption of the risk management standard, AS/NZS 4360:1999 (the second version of this standard) has facilitated this development, and has helped New Zealand and Australian organisations, both public and private, to be at the forefront of this development.

Risk management practitioners can hold out similar prospects for the use of risk management as many evaluation-related techniques. For example, the introduction to a risk management guide put out by the Aboriginal and Torres Strait Islander Commission (ATSIC) stated that:

'Risk management increases the prospect of ATSIC achieving its goals. The benefits of a sound risk management approach include:

- **better achievement of objectives**
  opportunities and threats are considered, operations are targeted on priorities, others are enlisted in the task
- **improved communication**
  inside and outside ATSIC about business directions
- **aiding good decision-making**
  through a forward-thinking approach, informed by lessons from the past, providing transparency and explicit criteria for choice
- **doing more with less**
  safeguarding resources, allowing them to be more closely targeted, with fewer costly surprises

- **good governance**
  in providing a means of management assurance
- **greater accountability**
  and
- **making decisions**
  which can be defended against criticism.**' (ATSIC 2001)**

Typical steps in a risk management process are stated as:

- Understanding the context
- Identifying the risks
- Assessing the risks
- Treating the risks
- Monitor and review

Understanding the risk has to be seen in the context of the wide definition of risk that is now adopted by the Standard, viz:

"The culture, processes and structure which come together to optimise the management of potential opportunities and adverse effects."

It should be noted that this new formulation of risk management attempts to go beyond the conventional interpretation of risk management as a means of minimising negative consequences by giving equal weight to potential opportunities. However, the author's view is that in practice risk management is still primarily a means of identifying and dealing with potential adverse events, although it can be the case that opportunity costs can also be dealt with by risk management.

The definition also emphasises concepts germane to evaluation such as the influence of culture on management, and understanding the context for decision-making.

The risk management approach to assessing risks relies conventionally on using a grid of likelihood and consequence, as below. An example of such a table is below:

Table 1 Determining the Level of Risk

Likelihood	**Consequences**				
	extreme	**very high**	**medium**	**low**	**negligible**
almost certain	severe	severe	high	major	significant
likely	severe	high	major	significant	moderate
moderate	high	major	significant	moderate	low
unlikely	major	significant	moderate	low	very low
rare	significant	moderate	low	very low	very low

In this way, a long list of identified risks can be ranked in order of significance for treatment.

Comparison between risk management and performance ,management

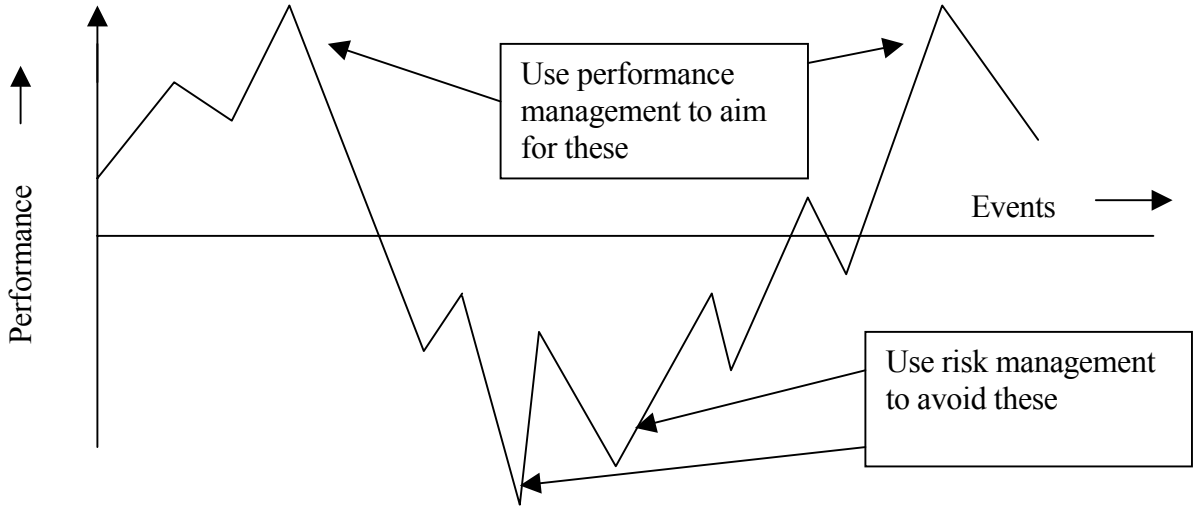
The following table indicates key similarities in the two approaches.

Table 2 Comparison between Risk and Performance Management

Risk management.	**Performance management**
A structured approach is undertaken to identify adverse events, and means of dealing with these so as to achieve business success. This includes:	A structured approach is undertaken to identify ways of measuring and achieving business success. This includes:
• Setting the context	• Defining the overall business goals and vision
• Identifying risks	• Identifying specific short-term targets
• Assessing the likelihood and criticality of each risk	• Selecting a feasible number of targets that, together, will span the business activity and therefore represent overall performance
• Overall assessment and ranking of risks	• Determining, where possible, the level of achievement against those targets to aim for
• Selection of treatments to apply to risks	• Allocate responsibility for achieving the targets, or at least monitoring performance
• Allocation of management controls to ensure treatments are applied	• Assess performance against targets regularly, and adjust management policies where appropriate
• Continuous review of risks to delete irrelevant ones and consider new risks.	• Reconsider regularly the relevance and appropriateness of the performance indicators

While there is not a strict one-to-one correspondence between the two activities, there are nevertheless considerable similarities. Indeed, one may consider risk management and performance management to be negative and positive aspects, the valleys and the peaks, of the same performance measurement issue, as depicted below.

Figure 1 Risk and Performance Management



Examples

The following examples add details to the sketch diagram above.

A program may have financial objectives, for example to achieve sales, profit or turnover objectives. The can be managed as performance objectives. At the same time, there may be risky activities that have possibilities of substantial losses that need to be put analysed using risk management approaches.

Sometimes the positive and negative aspects may be not as easily measurable, but still be broadly in the same dimension. For example, a program of physical works designed to address environmental remediation may also have potential adverse environmental consequences.

Finally, the performance targets and risks may be in different dimensions. For example, an expedition or field trip may achieve its scientific objectives, but still have significant OH&S risks.

Other similarities in the disciplines

Some other attributes of the risk management and performance management that are similar are described below.

The desire for quantification allied to the difficulty of doing so.

Risk management as defined in AS/NZS 4360: 1999 emphasises a qualitative description of risks, such as 'unlikely' likelihood, 'high' consequence or 'moderate' risk. The predefined levels aid in a semi-qualitative calculus whereby, for example, medium consequences multiplied by almost certain probability leads to high risk.

AS/NZS 4360 does not mandate such a schema, including a grid only as an example. Nevertheless, the example has had considerable force, with it or similar qualitative grids being used in most implementations of risk management.

For performance indicators there is a best practice advice to attempt to set quantitative indicators, together with target levels that are to be achieved. However, it can be difficult to suitably define such indicators, especially when a performance management system is first implemented.

Quantitative risk management is essential, of course, in industries such as insurance and investment, where potential losses can be defined in dollar terms, and it is necessary to estimate, based on past history or similar methods, the percentage likelihood of the event occurring. It is of value to attempt to use quantitative measures wherever practicable, as this gives a better understanding of the magnitudes of expected risk events.

Insurance and investment risk analysis each uses advanced mathematical methods, such as assessing 'beta' factors in a highly mathematical approach to reducing investment risks. The AS/NZS 4360 approach, by contrast, relies on descriptive terminology such as 'low' probability or 'catastrophic' consequence. A middle way of incorporating more numeracy into the user-friendly AS/NZS 4360 approach should be possible.

One approach is by using a method taken from evaluation, namely indifference models to assess consequence. This would involve asking decision-makers, 'Would you rather have this event happen, or lose $100 000? What if the loss were $1 000 000?' In this way, a dollar-equivalent measure of the adverse event can be estimated. The approach is still judgmental, but is more amenable to quantification.

Probability is, of course, inherently numerical and only requires to be set out in terms of a ratio or percentage. The downside is that most people tend to overestimate the likelihood of adverse events, so some background information is useful that describes the probability of particular incidents, (e.g. fire, flood, murder) so people can adjust their estimates.

Putting these two measures together would then allow more quantification of risk analysis. For example, the expected cost (value of event multiplied by its probability) before and after a risk treatment can be compered with the cost of the risk treatment to see if the treatment is cost-effective. There may be occasions where the risk reduction action is taken even if on average there are increased costs. For example, insurance policies on average are profitable for the insurance company, and therefore unprofitable for the policy-holder, but are still taken out because the expected cost is worth it to avoid the chance of damaging losses.

The need to integrate systems into general management approaches

In both cases, the main benefit of the approach is only gained when the work is integrated in to general management. Because there is the need to also include some specialist expertise in risk management or performance indicators in order to facilitate progress, there is a danger of adopting a stand-alone approach whereby responsibility is allocated to such specialists. This tends to reduce the value to the business, as line managers are best placed to identify risks, select performance measures and take the appropriate steps to minimise risk and enhance performance.

The problem of identifying intermediate and final outcomes

In both cases, there is the need to be logically rigorous about the distinction between causes and intermediate and final effects. The general principle is to aim for measuring as near as possible to final outcome, while recognising that sometimes this is not possible and therefore management relies on intermediate or proxy indicators or risks.

For example, one application of risk management to IT security considered the risk that a password is not kept secure. However, this is not a 'final' risk. The danger is that the lack of keeping the password secure might lead to the password falling in to the hands of an unauthorised person, and in turn that person uses the access to obtain confidential information which in turn is actually used to harm the interests of the organisation. The actual risk the organisation faces is the damage caused by misuse of confidential information. The presence or absence of password security is only a contributing factor, one link in the chain. In other words, it describes the presence or absence of a key control.

Similar considerations apply to performance indicators. In this case, evaluators are familiar with the causal chain of performance indicators often referred to as program logic. Program logic defines the sequence of causal factors from inputs through outputs, intermediate products, final products, outcomes and goals.

The National Action Plan on Salinity and Water Quality (NAP) is a joint activity of the Australian Departments of the Environment and Heritage, and Agriculture, Fisheries and Forestry. NAP developed a complex structure of inputs leading in turn to activities, outputs, short term, medium term and long term outcomes, thence to broad outcome areas, NAP goals and finally Natural Resource Management (NRM) Output objectives.

The difficulty of measuring the eventual objective is recognised, and therefore in many cases it is accepted, albeit reluctantly, that one has to measure and report on intermediate or lower level objectives in order to obtain timely feedback on the progress of a program.

Such a hierarchy of events should also be explicitly considered in risk management. In other words, if the final risk is not easily measurable or controllable, managers should measure and control the risk factors that are likely to lead to that final risk event occurring.

In such cases, it is necessary to be clear about what one is measuring, and not duplicate or overstate risks when they re actually part of the one chain of causality or influence. To return to the IT security example, the risk manager may decide that the final risk of damage through loss of information is too difficult to measure or control, and therefore one of the risks to be analysed is the intermediate risk of loss of password security. For this risk, the likelihood that at least one password throughout the organisation is compromised may well be high. But the consequence is not as severe as damage through loss of sensitive information, as for that to happen, several other adverse events must occur. An assumption that loss of password security is the same as loss of confidential information would lead to too high a risk rating, and hence the possibility of wrong decisions.

The problem of setting levels to achieve or avoid

For both performance indicators and risk events, the organisation must decide what level of performance to aim for or what level of risk to avoid. In the case of performance information, this is a well recognised issue, with the setting of achievable but demanding targets being considered features of a good performance measurement system. However, many of the performance indicators and results published do not set clear target levels – for example much of the performance reporting by Commonwealth Government Departments (ANAO 2001)

Some performance indicators fail this test simply because they are expressed in qualitative terms, e.g. the extent to which the Minister's expectations are met. The invariable response is 'to a high degree' or similar. Even when the performance measure is quantifiable, the target performance level is not always set.

For performance indicators, this issue is recognised, even if the practice sometimes falls short of theory. For risk management, it is not even a well recognised issue.

For example, a risk to a project might be that a key subcontractor delivers late. How late? One day or many months? One has low consequences, the other low probability. Which should be analysed, or should several potential risk events be considered?

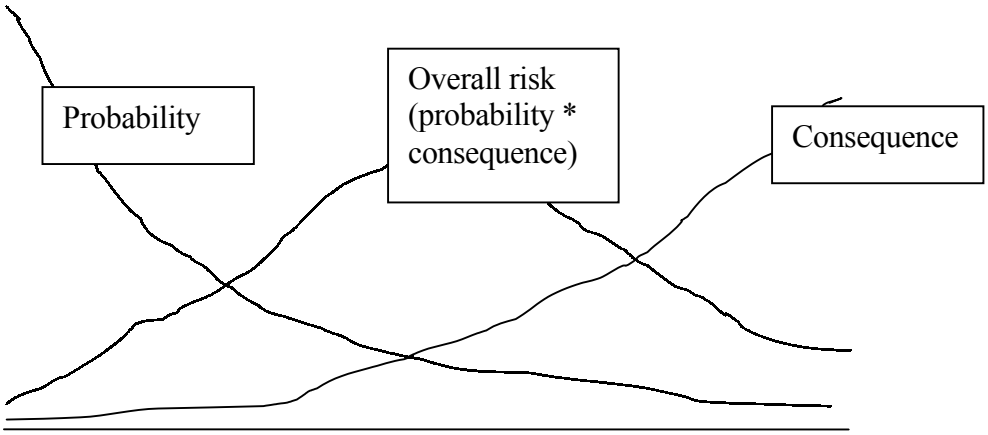
The total penalty for this risk can be presented mathematically as:

$$R = \int_{x=0}^{x=\infty} (p(x).c(x)dx$$

where R is the overall risk, p(x) is the probability of a lateness of x days, and c(x) is the consequence of that lateness.

This is illustrated in Figure 2 below:

Figure 2 Overall Risk for a continuous variable



The integral calculates the total risk as depicted above by the area under the risk curve. However, this is not normally a function worth calculating, as there is often little detailed information on either probability or consequence, and so the functions would only be judgmentally determined.

An approximation of this calculation is to consider the cumulative probability multiplied by the consequence that attains to that probability. An example of this, using the contract lateness example mentioned earlier, is depicted in the following table:

Lateness of x days or more; X=	Likelihood	Consequence (e.g. liquidated damages for lateness of project)	Risk (product of likelihood and consequence)
1	.95	1	.95
3	.8	5	4.0
10	.3	25	7.5
30	.02	200	4
100	.001	1000	0.1

In this simple example, the worst overall risk is that of a lateness of 10 days. This therefore becomes the risk level of interest. Although this is indicative of overall risk, this estimate is a lower bound to the risk as calculated earlier.

In practice, even this simplified calculation is often neither possible nor necessary. But it is often necessary, using judgement, to determine the appropriate level of risk to analyse. A reasonable principle is, as above, to choose the definition of risk level that, at least on a judgmental basis, produces the worst outcome.

A similar calculation can be used to determine what is the level of interest for a performance indicator; in this case, we would be interested in the proportion of sub-contracts for which delivery is less than ten days late.

Conclusion – combining risk and performance.

It is instructive to note that risk management is better structured to assess likelihoods and consequences of the outcome, while performance measurement is better at setting target levels and considering the chain of causality leading to achievement of that performance. Both facets of understanding are relevant to both forms of management information and control, and therefore there are opportunities for the disciplines of risk management and performance measurement to learn form each other.

It can also be seen that for risk management and performance measurement, there are some similar issues and difficulties, and similar approaches that can be taken to resolve these difficulties.

The issue of whether risk management and performance measurement can be fully integrated is more problematical. One approach is to take seriously the definition of risk in AS/NZS 4360, which refers to risk management covering not only adverse events, but also opportunities. The outcomes and goals to which performance management is directed can then be considered as 'opportunities' in a risk management context. For these events, we can use a risk management structure to define the probabilities and consequences of not achieving them.

Alternatively, the risk levels can all be set out in terms of performance targets. For example, there may be a lateness risk defined as a program being delivered more than seven days late. Instead, we could have a performance indicator of timeliness, with the measure being might be the proportion of programs delivered within seven days of the due date.

Neither of the above is totally satisfactory. Part of this is the different management emphasis that is understandably placed on avoiding disasters or achieving performance. Perhaps the best solution is an organisational one, to ensure that those parts of the organisation charged with coordinating risk management, and with collecting and managing performance information have close communication, or perhaps are the same group.

References

Australian National Audit Office, *Audit Report 18 of 2001-2, Performance Information in Portfolio Budget Statements*

Aboriginal and Torres Strait Islander Commission, *Risk Management Guideline - the 'Why Not?' of Risk Management* 2001 (internal document)

Standards Australia: Australia and New Zealand Standard 4360:1999 – Risk Management