Broadleaf

Creating value from uncertainty

Broadleaf Capital International Pty Ltd

ABN 24 054 021 117

www.Broadleaf.com.au

Tutorial:
Setting priorities for risk treatment and assurance of controls

In an organisational setting, risk assessment processes often identify many risks, but managers usually have limited time and resources available for dealing with them. Managers need to be able to set priorities to focus their attention on the areas where the application of effort will produce the most effective risk treatment and assure the effectiveness of controls.

Version 8, 2014

Broadleaf

Contents

1 Abstract 4

2 Background 5

3 Risk analysis 6

3.1 Simple analysis of levels of risk 6

3.2 Priorities based on levels of risk 7

3.3 Enhancing risk analysis 8

3.4 Control effectiveness 9

3.5 Potential exposure 12

4 Risk analysis, evaluation and treatment 13

4.1 General principles for evaluating treatment options 13

4.2 Developing treatment options 13

4.3 Consequences, likelihoods and level of risk 14

4.4 Control effectiveness and level of risk 16

4.5 Bow tie analysis 17

4.6 Benefits and costs 18

4.7 Optimisation 19

5 Risk analysis, evaluation and assurance 20

5.1 Potential exposure and level of risk 20

5.2 Assurance options 22

5.3 Inherent risk 23

6 Conclusions 24

7 References 25

8 Contact 26

Tables

Table 1: Control effectiveness rating scale 10

Table 2: Control effectiveness and level of risk 17

Table 3: Level of risk and potential exposure 22

Table 4: Summary of indicative priorities from extended risk analysis 24

Figures

Figure 1: Characteristics of a metric for estimating level of risk 7

Figure 2: Focus of risk treatment 8

Figure 3: Potential treatment actions for risks with detrimental consequences 15

Figure 4: Treatment and assurance actions based on control effectiveness and level of risk 16

Figure 5: Bow tie analysis structure 18

Figure 6: Treatment and assurance actions based on potential exposure and level of risk 21

1 Abstract

In an organisational setting, risk assessment processes often identify many risks, but managers usually have limited time and resources available for dealing with them. Managers need to be able to set priorities to focus their attention on the areas where the application of effort will produce the most effective risk treatment and assure the effectiveness of controls.

The main formal output of common-practice risk assessment is a level of risk, based on an analysis of the consequences of the risk, given existing controls, and the likelihood of those consequences arising. However, this only provides crude priorities for attention, and the level of risk by itself does not provide much information about appropriate treatment or assurance options or which ones to address first.

As well as consequences and likelihood, two additional measures are particularly useful: control effectiveness and potential exposure. Control effectiveness measures the design adequacy and the effectiveness of the implementation of the controls that are intended to modify a particular risk. It is a useful precursor to estimating consequences and likelihoods. Potential exposure is the maximum consequence to which the organisation may be exposed if all the controls were to fail; it is a measure of consequences only.

With these two additional measures, the risk analysis process yields five measures for each risk: control effectiveness; a consequence measure for the risk, with the current controls; the likelihood of the selected magnitude of consequences arising with the current controls; the level of risk, derived from a combination of the consequence and likelihood measures; and potential exposure. This paper explores how combining these measures in different ways generates useful guidance for setting priorities for managers' attention to and decisions about treatment actions and assurance.

Key words: assurance of controls; audit; bow tie analysis; consequences; control effectiveness; inherent risk; ISO 31000; level of risk; likelihood; potential exposure; risk assessment; risk management; risk treatment

2 Background

In an organisational setting, risk assessment processes often identify many risks, but managers usually have limited time and resources available for dealing with them. Managers need to be able to set priorities to focus their attention on the areas where the application of effort will produce the most effective risk treatment and assure the effectiveness of controls.

Common-practice risk assessment focuses on generating a level of risk, based on analysis of the consequences of the risk, given existing controls, and the likelihood of those consequences arising. However, this only provides crude priorities for attention, and the level of risk by itself does not provide much information about appropriate treatment or assurance options or which ones to address first.

This paper explores priority setting in risk assessment and how the approach can be enhanced relative to the basic practices that are commonly used. It uses definitions and concepts based on ISO 31000 (ISO, 2009):

- Risk is defined as the effect of uncertainty on objectives;
- A risk may have many consequences, it can affect many objectives, and the consequences for those objectives may be beneficial or detrimental;
- Risk assessment is the overall process of risk identification, risk analysis and risk evaluation;
- Risk analysis is concerned with developing an understanding of the risk; it should generate a range of information including levels of risk, taking the current controls into account;
- Risk evaluation is the step in which decisions are made, based on the outcomes of the risk analysis, to decide which risks need priority attention; and
- Risk treatment involves selecting and implementing options for modifying risk.

In practice it takes time and resources just to identify potential treatment options and their associated benefits and costs, let alone implement the treatments. The risk management process can absorb a lot of effort or be prematurely curtailed by concerns about the amount of effort required simply to determine what treatments should be pursued.

There are usually many options for treating a particular risk, and often it is appropriate to implement more than one option if there are several that offer a

net benefit to the organisation. It is important to allocate resources purposefully, including resources applied to the identification and analysis of treatment options and the development of treatment plans, to optimise the use of resources.

Most organisations have well-established control processes. The enhanced risk assessment process described here also assists in the identification of key controls and setting priorities for assurance activities, including the development of assurance and audit plans. It is important that the excitement of treating significant risks does not result in well-controlled risks being overlooked to the extent that controls are weakened.

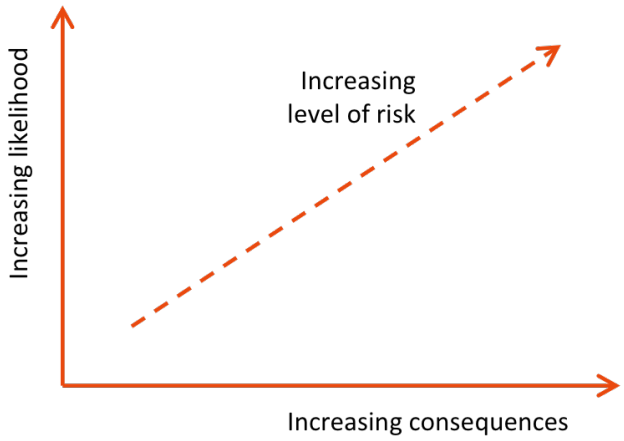
3 Risk analysis

3.1 Simple analysis of levels of risk

Common-practice risk assessment (based on ISO 31000 or equivalent standards) is focussed on generating a level of risk, based on assessments of the consequences chosen to characterise the risk, given the controls in place and their effectiveness, and the likelihood of those consequences arising. It is often proposed that the levels of risk, derived in some way from measures of consequences and likelihood, be used for setting priorities for attention for risk treatment activities or for deciding what are 'acceptable', 'tolerable' or 'unacceptable' levels of risk.

No matter how it is derived, the level of risk should increase as consequences or likelihoods increase (Figure 1), but otherwise its characteristics are not critical for the purposes of this paper.

Figure 1: Characteristics of a metric for estimating level of risk



It is worth noting that metrics for generating levels of risk are generally not as easy to create as their apparent simplicity might suggest. Taken together, the scales for measuring consequences and likelihoods and the manner in which they are combined in the risk metric reflect the risk attitude or risk appetite of the organisation within which they are applied. A coherent and agreed perspective of an organisation's risk appetite (or risk attitude) is essential if risk management is to support and integrate with other management processes. Developing scales and levels of risk is a challenging, subtle and iterative process. There is no substitute for experience if a clear and useful outcome is to be achieved.

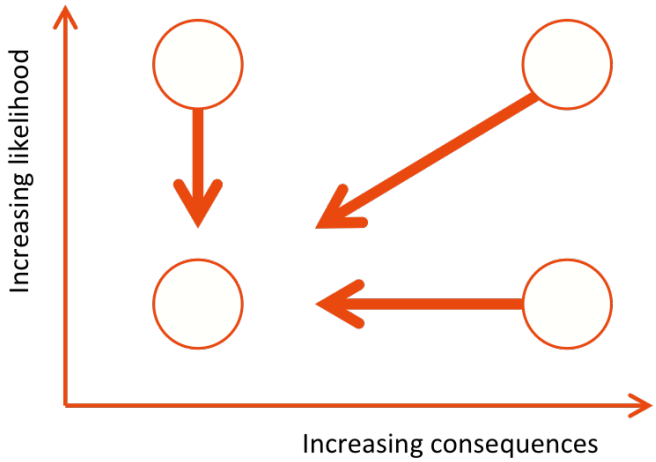
3.2 Priorities based on levels of risk

Common-practice risk assessment based on consequence and likelihood measures generates levels of risk. It then ranks risks according to the level of risk, from high to low. This provides a very crude priority for attention.

The level of risk by itself does not necessarily indicate a need for risk treatment. Organisations should not take actions just because the current level of risk is large. They should only act if there is an organisational benefit from doing so (unless, of course, there are regulatory or policy requirements that over-ride net benefit considerations). Any priority-setting process should take account of the cost-effectiveness of potential treatment options (see, for example, Cox, 2012). An important corollary of this statement is that a change in the level of risk is not the only measure of benefit for a risk treatment action. The main criterion should be the net effect on the organisation bearing the risk.

In addition, the level of risk does not provide information about what treatment options might be most appropriate or even whether treatment could be beneficial or not. There may be risks with a high rating for which no further action is justified, unless it is to abandon the course of action through which they come into being. Conversely, there may be low-level risks where treatment would have a net beneficial effect. The consequence and likelihood measures that underlie the level of risk indicate the kinds of treatment options that may be appropriate: change the likelihood for risks in the top-left of Figure 2 or change the consequences for risks in the lower-right. (Note that changing the likelihood may include options that reduce the likelihood to zero, for example by avoiding the risk altogether or doing something different.)

Figure 2: Focus of risk treatment



Despite the insight that is offered by keeping the consequence and likelihood ratings in view, much better guidance can be provided to decision-makers using two simple additional measures for each risk.

3.3 Enhancing risk analysis

As well as measures of consequences, likelihoods and levels of risk, two additional measures have been found to be particularly useful: control effectiveness and potential exposure. These impose almost no additional burden on the risk assessment process but yield significant value.

The level of risk is measured in the context of existing controls and their level of effectiveness. Control effectiveness measures the design of the set of controls that act to modify a particular risk (their adequacy) and the effectiveness of their implementation. It is not assessed individually for each control but for the

assembly of controls associated with a risk. Not only is this useful in later analysis, considering control effectiveness before estimating consequences and likelihoods makes the analysis run more smoothly and informs and influences the analysis of consequences and their likelihoods. It draws the attention of participants to this crucial aspect of the analysis, the effectiveness of the controls relative to what is reasonably practicable.

The second additional measure is potential exposure. Potential exposure is the total plausible maximum consequence the organisation could experience if all the controls were to fail or were absent. It is a measure of consequences only and, in conjunction with a level of risk, it provides valuable guidance about how important it is for a risk to be treated and for controls to be present and effective.

We now have five measures that come from the risk analysis process for each risk:

1. Control effectiveness;
2. A consequence measure for the risk, with the current controls and their level of effectiveness;
3. The likelihood of the selected magnitude of consequences arising, with the current controls and their level of effectiveness;
4. The level of risk, derived from the consequence and likelihood measures; and
5. Potential exposure.

Generating measures of control effectiveness and potential exposure in a risk analysis takes very little additional effort. By contrast, combining all five generates very valuable information about where the priorities for management attention should lie.

3.4 Control effectiveness

A control is anything that modifies risk; controls may include existing policies, devices, procedures and practices. The level of risk is estimated taking into account the context and the environment in which the organisation currently operates and the controls that are in place. However, existing controls may not all be well designed, they may not all be well implemented and they may not operate as intended when required. These are the factors measured by control effectiveness.

Control effectiveness takes into account both the adequacy of the controls and how well they are implemented. Adequacy refers to the design of the controls and whether they would achieve the desired control outcomes if they were implemented well; implementation refers to how well the controls are executed in practice as well as their availability and reliability when they are needed. The control effectiveness measure is only applied to the suite of controls that are relevant for a risk, rather than attempting to apply it to each control, which is not useful. It is a measure of the completeness, relevance and efficacy of all the current controls operating on a risk.

Control effectiveness is a relative measure that estimates the actual level of control that is currently present and effective compared with that which is reasonably achievable by the organisation for a particular risk. It does not refer to perfect control, which is an unrealistic and meaningless concept.

When conducting a risk analysis, it is useful to assess the effectiveness of the controls before assessing consequences and likelihoods. This can bring out useful insights and promote valuable communication among the risk assessment participants. An example of a control effectiveness rating scale is shown in Table 1 (adapted from Finger et al, 2010).

Table 1: Control effectiveness rating scale

Control effectiveness	Guide
Fully effective	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, and address the root causes. Management believes they are effective and reliable at all times.
Substantially effective	Most controls are designed correctly and are in place and effective. Some more work to be done to improve operating effectiveness or management has doubts about operational effectiveness and reliability.

Control effectiveness	Guide
Partially effective	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. or Some of the controls do not seem correctly designed in that they do not treat root causes. Those that are correctly designed are operating effectively.
Largely ineffective	Significant control gaps. Either controls do not treat root causes or they do not operate at all effectively.
None or totally ineffective	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design or very limited operational effectiveness.

It is important to note that control effectiveness as defined here is measured in relation to what the organisation could do, not in relation to a hypothetical state of perfect control. It is a measure of organisational and managerial effectiveness.

An organisation's controls may already be as good as it is reasonably able to make them (taking into account its circumstances and its risk appetite as well as the characteristics of the risk). In these circumstances, control effectiveness would be rated high, even though high natural or external variability that cannot be controlled may remain, with a corresponding high level of risk. For example, an organisation may have excellent treasury functions, and hence high control effectiveness on exchange rate and interest rate risks, yet still regard volatility in foreign exchange rates, interest rates and commodity prices as a high risk to its profitability.

The additional information provided by control effectiveness can highlight areas that warrant attention. Where control effectiveness is less than 'fully effective' consideration should be given to risk treatment that further modifies the risk, either by adding new controls, improving the design of the existing controls or increasing their effectiveness, availability and reliability. This is particularly important if the level of risk is high. Whether particular treatments are actually implemented will depend on whether they are cost-effective or have a net

beneficial effect not only on financial measures but also other factors such as safety, public relations and other intangible but important objectives.

3.5 Potential exposure

Potential exposure a simple but extremely useful measure of a risk. It is the maximum consequence to which the organisation may be exposed if all the controls were to fail in a plausible manner. It is a much more effective means of assessing how severe a risk could be if it was uncontrolled than the troublesome concept of inherent risk, as explained later in this paper. Potential exposure achieves what inherent risk was intended without the conceptual and practical problems that inherent risk entails.

Some risk analysts use the term 'exposure' in very specific ways. For example exposure to drugs, toxins and so on is a different use of the word that should not be confused with potential exposure. Although we use the term potential exposure, other terms for the same concept include maximum foreseeable loss (e.g. in insurance applications) or maximum potential consequences. These all share the properties of being free from any consideration of likelihood and framed by the plausible failure of controls.

Potential exposure is measured in terms of consequences only.

- If a single measure of consequences is used by the organisation, say dollars, then potential exposure is the maximum monetary loss associated with the risk if all the controls were to fail. This might include direct costs (like repair costs, fines or compensation payments), indirect costs (like business disruption and reestablishment costs), and opportunity costs (like lost profit or reduced growth potential). In this case, potential exposure can be measured on a numerical ratio scale denominated in dollars.
- Some organisations use two measures of potential exposure: one based on monetary value and another based on safety outcomes such as fatalities or morbidity.
- If the organisation is using an agreed set of consequence scales for its risk analysis, possibly including financial, timing and intangible measures, then a potential exposure rating can be based on those same consequence scales. If an ordinal (ranking) scale is used for consequences, such as is commonly employed in qualitative risk assessment, then potential exposure can be measured on an ordinal scale.

Potential exposure is used to identify key controls. A key control is a control or group of controls that is believed to be maintaining an otherwise intolerable

risk at a tolerable level. If such controls fail, the consequences can be, by definition, intolerable.

4 Risk analysis, evaluation and treatment

Risk assessment has little value unless it leads to action. Formulating and selecting treatment actions is a key part of delivering value from the assessment.

4.1 General principles for evaluating treatment options

The level of risk alone does not mandate or require that action be taken, except in specific circumstances that are defined by regulation or set by organisational policy. A high risk rating by itself does not necessarily mean that risk treatment is warranted.

In most circumstances, action should only be taken if the benefits for the organisation exceed the costs. Note that the calculation of benefits and costs must be interpreted comprehensively – benefits and costs in this context should not be thought of only in terms of money. Any significant benefit or detriment associated with implementing a treatment, whether financial or not, tangible or intangible, should be taken into account.

The evaluation may be adjusted for risks with safety-related consequences, to encompass criteria based on concepts like ALARP (as low as reasonably practicable) or SFAIRP (so far as is reasonably practicable). These criteria are still based on the comparison of benefits and costs, but they require that risk treatment must be implemented unless the costs are disproportionate compared with the benefits.

4.2 Developing treatment options

Options may be developed from generic treatment strategies, with additional information derived from the risk analysis, or as entirely original actions based on a fresh consideration of the challenge that they present. Generic treatment strategies include:

- Do something different, to avoid the risk with detrimental consequences;

- Do something different to increase the risk with beneficial consequences;
- Change the likelihood (often embedded in business processes, e.g. preventive or directive controls);
- Change the consequences (e.g. detective or corrective controls, contingency planning);
- Share the risk (e.g. contractual controls, insurance); or
- Accept the risk without further treatment.

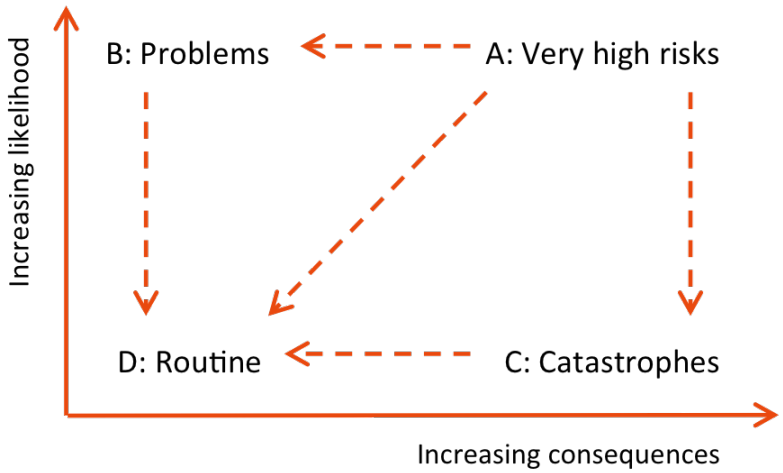
Technical and domain expertise will usually be brought to bear in developing treatments. Innovation and ingenuity may throw up fresh ideas or expose options that are specific to the system to which the risks apply, independent of generic approaches.

4.3 Consequences, likelihoods and level of risk

Risk ratings, the measure based on the combination of consequences and likelihood, are the initial and often the most important guides for setting priorities for decisions. Risks with high ratings are usually those with high consequences and high likelihoods of those consequences arising. They usually merit management attention with the intent of evaluating possible actions to reduce the level of risks with detrimental consequences (the threats) or to exploit those with beneficial consequences (the opportunities).

The consequence and likelihood measures provide a guide to the kinds of treatment responses that may be relevant for each risk. Figure 3 illustrates the analysis for risks with detrimental consequences or high likelihoods; the arrows indicate the direction of desirable changes.

Figure 3: Potential treatment actions for risks with detrimental consequences



A general guide to treatment strategies is outlined below for each of the four characteristic assessments shown here.

A. Very high risk area. Detailed attention should be paid to risks in this area, and risk treatment action is usually warranted. This may be directed to changing the likelihood of the consequences (or avoiding them altogether), or changing the consequences, or both. In Figure 3, this would have the effect of moving the level of risk to the regions labelled B, C or D.

B. Problem area. Risks in this area have high likelihoods but moderate to low consequences. Treatment actions might focus on improving management systems and procedures that reduce the likelihood of problems arising. Two practical difficulties arise in this area: the first is that frequent recurrence results in complacency and an under-allocation of attention and resources devoted to permanent solutions; the other is that the high frequency of recurrent consequences, or the perceived imminence of those that do not recur but are felt to be highly likely, leads to excessive management attention and an over-allocation of resources.

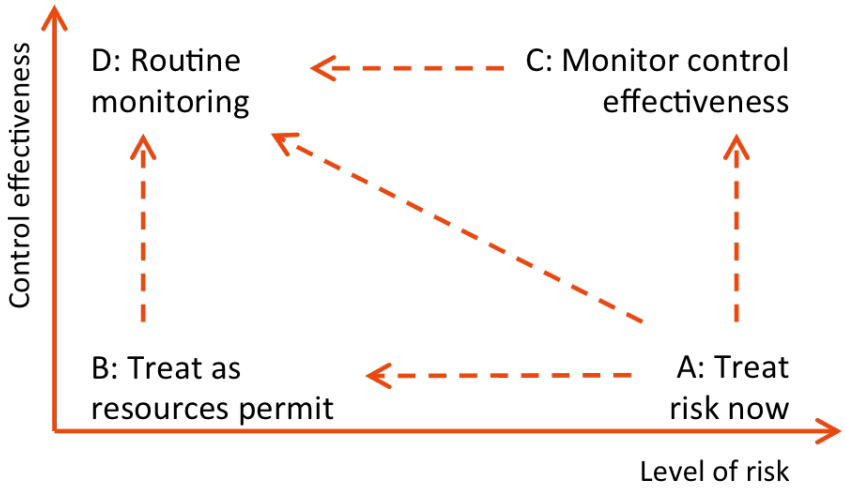
C. Catastrophe area. Risks in this area have low likelihoods but potentially high consequences. Effective preparation and contingency planning such as business continuity management are often valuable options for these risks. Insurance or other forms of contingent capital may be appropriate. Because of many organisations' aversion to high consequence events, managers should ensure that this area receives adequate resources even though the priority may seem less urgent.

D. Routine area. Established processes, systems and procedures often control risks in this area already. If not, simple measures are usually sufficient to ensure that they remain relatively insignificant.

4.4 Control effectiveness and level of risk

Within a group of risks with high ratings, those with low control effectiveness merit particular attention. Where controls are recognised as less than ideal and capable of improvement it almost goes without saying that options for improvement should at least be considered. Control effectiveness ratings complement levels of risk for setting priorities for consideration of treatment. Figure 4 and the detailed descriptions that follow it outline the implications of these ratings for risk treatment and assurance planning.

Figure 4: Treatment and assurance actions based on control effectiveness and level of risk



A. Here there are high levels of risk with controls that are not fully effective. Treatment actions should be implemented soon, to reduce threats and exploit opportunities. These actions are likely to generate new or improved controls, or to improve the effectiveness of existing controls.

B. Low levels of risk for risks with controls that are not fully effective. They may have large consequences that are unlikely to occur, or low consequences that are highly likely. Treatment actions should be implemented as resources permit.

C. High levels of risk for risks with effective controls so that further action is unlikely to yield any benefits. These controls are effective but the level of risk remains high. Formal assurance processes to monitor control

effectiveness are recommended, as well as routine control reviews (such as control self-assessments and audits). Environmental scanning may be worthwhile to detect material changes to risks or triggers for events that could lead to threats or opportunities.

D. Low levels of risk for risks with effective controls. Routine monitoring and review of controls is recommended.

Table 2 shows an example from a recent case study. The priority area for control improvement is highlighted. The numbers in the matrix show the number of risks falling in each cell.

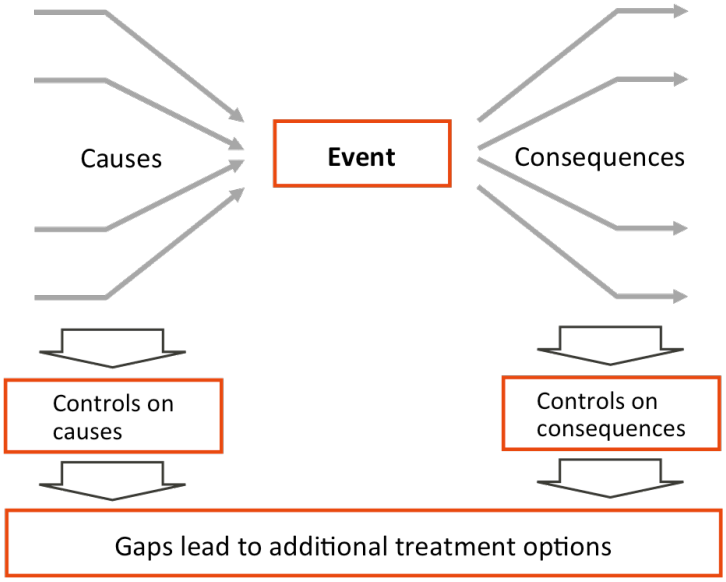
Table 2: Control effectiveness and level of risk

		Level of risk			
		Low	Medium	High	Extreme
Control effectiveness	Fully effective		9	8	2
	Substantially effective		22	44	12
	Partially effective		9	42	22
	Largely ineffective		4	12	15
	None or totally ineffective			5	2

4.5 Bow tie analysis

Bow tie analysis (Figure 5) may assist in identifying specific areas of control weakness or where controls might be added or enhanced usefully. Bow tie analysis augments the analysis described in the previous section by providing further detail about causes, consequences and the existing controls that act on the causes and consequences. The specific gaps in controls that this method exposes indicate where and what kind of additional treatments might be appropriate, for example to develop new controls or to enhance existing controls that will fill the gaps more effectively.

Figure 5: Bow tie analysis structure



4.6 Benefits and costs

Organisations undertake risk treatment to reduce uncertainty about whether they will achieve their objectives and to what extent they might fall short. Decisions about risk treatment should not be based on the ratings of specific risks alone, but on the best outcomes for the organisation and its objectives, usually measured in terms of net benefits and costs.

As one treatment can affect more than one risk, benefits and costs should take into account all the benefits and all the costs across all risks, not just the benefits and costs associated with a particular risk that led to or prompted the identification of a risk treatment option. At this stage in the analysis, a holistic approach is imperative.

The estimation of benefits and costs should take into account all the direct and indirect benefits and costs, monetary, tangible and intangible. They will usually not all be measurable easily in financial terms. A change in the level of risk is rarely the only measure of benefit for a risk treatment action, and some actions may be desirable even if the change in the level of risk is small, as no risk-rating scheme is absolutely comprehensive and exhaustive. The insights gained from the analysis might include valid reasons for pursuing treatments that are not simply directed at the most severe risks.

There are two circumstances in which analysis of benefits and costs alone is not sufficient or appropriate for guiding decisions about whether or not to implement a treatment. Firstly, where there is a legal or regulatory requirement, or a corporate policy imperative, action may have to be taken irrespective of the associated costs. Secondly, where there are consequences related to the safety of people, criteria like ALARP (as low as reasonably practicable) or SFAIRP (so far as is reasonably practicable) usually apply, and these require treatment actions to be undertaken unless the costs are very large and disproportionate compared with the benefits.

4.7 Optimisation

Most organisations have constraints on capital and other resources for implementing treatment and assurance actions. Ideally, resources should be allocated simultaneously across many treatment and assurance options, portfolio-wide rather than for separate risks independently, to optimise the net benefit for the organisation within the constraints of the available resources.

For example, this optimisation might be formulated as:

$$\text{Maximise net benefit } B = \sum_{i=1}^{N} J_i \, b_i$$

$$\text{subject to } \sum_{i=1}^{N} J_i \, c_i \leq C$$

where there are N options i, b_i is the net benefit to the organisation from implementing option i, c_i is the cash cost of implementing option i, C is the total cash pool available and $J_i = 1$ if option i is implemented, 0 otherwise.

Full portfolio-wide assessment of capital allocation to risk treatments requires significant effort to be expended on the initial identification and analysis of options, which means it will rarely be possible to identify a full set of N feasible options. In these circumstances the (sub-)optimisation may focus on a subset of n credible options, where n is fewer than N. Some of the priority-setting approaches described in this paper may be useful for selecting the subset of options by directing attention to those areas where actions might be most valuable.

Such formulations can be expanded to allow for options that interact, or are mutually exclusive, or to incorporate constraints on more than one class of resource.

Cox (2012) addresses the allocation of limited budgets to risk-reduction options where benefits are expressed in terms of reductions in a one-dimensional measure of risk. He shows that a heuristic rule of 'address the largest risk reductions per unit cost first' until the budget is expended – equivalent in the formulation above to implementing the options with the largest b_i/c_i ratios while there is cash available – is better than other comparable rules, at least for cases where the budget is sufficient to implement a reasonably large set of options.

5 Risk analysis, evaluation and assurance

5.1 Potential exposure and level of risk

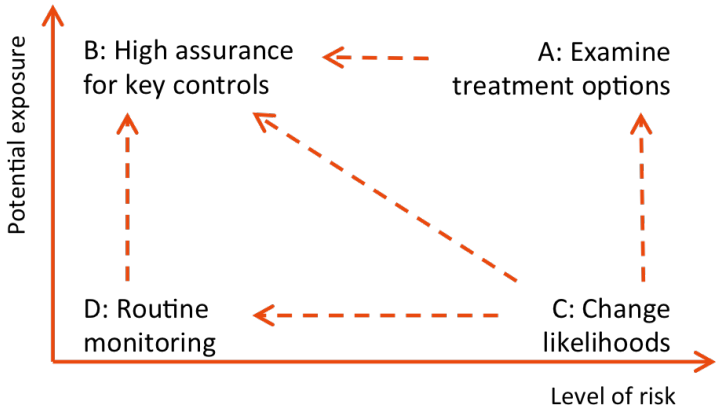
Potential exposure provides a guide to where control assurance is important. It is most critical where the potential exposure is high and the level of risk is low. In these circumstances, a loss of control can be expected to result in major consequences being felt.

This is particularly important where the reason that managers expect the level of risk to be low is because they believe that existing controls are fully or substantially effective. In these circumstances a high potential exposure indicates very significant consequences if the existing controls do not work as intended or are not as effective as expected. The controls that are assumed to be modifying the risk so that the level of risk is low are the 'key controls'.

Key controls should be the primary focus for control monitoring and review activities. They should be allocated to named 'control owners' who are responsible for planning their assurance. Assurance of this kind generally includes the continual monitoring of indicators that reflect the health of the control and give early indications of weakness, supplemented by periodic and complementary review activities including control self-assessments, reviews or audits. The objective is to provide assurance to the risk owner that the controls continue to be effective.

Figure 6 and the detailed descriptions that follow outline the implications of these measures for risk treatment and assurance planning.

Figure 6: Treatment and assurance actions based on potential exposure and level of risk



A. High levels of risk for risks with high potential exposures. These risks have consequences that are potentially large and are likely to arise. Treatment actions to improve controls should be implemented soon. In this case, potential exposure acts as a secondary indicator of priority: review the high risks first (for example, following Figure 3), and within the high risks, review those with high potential exposures first.
B. Low levels of risk for risks with high potential exposures. Here the level of risk can only be low if the controls are effective; were the controls to fail, the high potential exposure could lead to a significant impact on the organisation. Rigorous monitoring and review of controls are required for the risks here.
C. High risks with low potential exposures. Consequences are low, even if the controls fail, so treatment actions directed to changing likelihoods are required.
D. Low risks with low potential exposures. Routine control self-assessments and less-formal or less-frequent assurance processes may be recommended.

Area B in Figure 6 is particularly important. For a risk in this area, the level of risk is low, so it might be tempting to assign this risk a low priority for attention – after all, it has a low level of risk. However, the high potential exposure rating means that the consequences for the organisation would be large were the controls to fail; in other words, the controls and their continuing effectiveness are very important for achieving organisational objectives – in audit terms these are key controls. The organisation and its governing bodies need to obtain assurance that the key controls are present and effective and will be available when required. They are likely to require formal, periodic reviews such as

independent audits, control self-assessments and continual monitoring to maintain a high level of confidence in the controls.

Although it may seem counter-intuitive to direct assurance efforts towards the risks with low levels of risk, that's where the key controls are. It is the key controls that are expected to modify these risks to a low level of risk that should form the basis for assurance and audit planning, rather than those in area A. Managers should already know about the risks in area A and be addressing them through risk treatment as risks in this area naturally attract attention.

Table 3 shows an example from a recent case study. The priority area for monitoring and assurance of controls is highlighted. As in Table 2, the numbers in the cells represent the number of risks in each cell.

Table 3: Level of risk and potential exposure

		Level of risk			
		Low	Medium	High	Extreme
Potential exposure	5		20	71	52
	4		9	31	1
	3		11	9	
	2		4		
	1				

5.2 Assurance options

There are several levels of assurance process, listed here in generally decreasing order of effectiveness.

- Controls that are built in to day-to-day processes and methods of work and thus are monitored continually.
- Periodic but frequent review by line managers, often called control self-assessment.
- Periodic but less frequent assurance by independent assurance providers outside the direct organisational line of the control owner, such as internal audit (whether undertaken internally or by an outsourced provider) or external audit (but often with restricted scope in terms of the controls that are examined).

Potential exposure and level of risk together provide a guide for those areas where assurance activities may be warranted.

- Key controls identified in a risk analysis process like that in Figure 6, using measures of potential exposure and level of risk, should be the main priority for assurance activities of all kinds, and a primary guide for planning audit activities. Control owners should be responsible for planning and implementing assurance activities, particularly monitoring, while an audit or finance function may direct audit activities.
- Areas of risk where the control effectiveness measure from Table 1 indicates improvement possibilities should be the focus for risk treatment, which should be the responsibility of risk owners.

5.3 Inherent risk

In the past, the concept of 'inherent risk' has been used as the basis for assurance planning. Potential exposure replaces inherent risk, a term is not used in the international standard ISO 31000.

Inherent risk is often used in an accounting sense as the risk of a material accounting misstatement assuming there are no related controls. This is just one definition of inherent risk though. Other definitions include:

- The risk that is inherent in the business environment in which the organisation operates;
- A risk that cannot be managed or transferred away;
- The level of risk without any controls at all (sometimes called 'naked risk');
- The level of risk without some controls (typically without tangible controls like policies and procedures, but assuming 'inherent' controls like common sense remain in place);
- The risk that is related to natural variability, as opposed to specific events or circumstances.

The lack of a clear definition is just one of the problems with inherent risk. The other is that the whole notion of an environment without controls has little practical meaning for most people – it does not make sense. While it may be possible to assess the consequences of a risk in an environment without controls or where the controls fail, it is very difficult both to estimate and to validate the likelihood of those consequences to arrive at an inherent level of risk.

Potential exposure provides the same outcomes for assurance planning as inherent risk is intended to deliver but it is easier to define, understand and

estimate in practice. In contrast to inherent risk, potential exposure relates to tangible 'worst-case' consequences that people can imagine or visualise and for which they can construct credible scenarios. They can make consequence estimates with more confidence and the difficulty of estimating likelihood for an artificial circumstance is avoided. This is demonstrated in practice.

6 Conclusions

Setting priorities for attention should take into account all of the information available. Simple analysis of consequences, likelihoods and levels of risk is rarely sufficient. Other measures from the risk assessment, and particularly control effectiveness and potential exposure, provide essential additional guidance.

Outcomes are not just related to risk treatment actions, but also to assurance activities that ensure controls remain effective. These two areas together flesh out the otherwise sparse focus of risk assessment on high risk ratings.

Table 4 shows indicative priorities from the preferred approach to risk analysis discussed in this paper. Setting priorities is not a rote, mechanical process, and the information discussed here is only a guide – it is not a substitute for sound thinking by managers.

Table 4: Summary of indicative priorities from extended risk analysis

Level of risk	Potential exposure	Control effectiveness	Priority for treatment action	Priority for assurance activity
High	High	Low	1	2
		High	4	
	Low	Low	2	3
		High	5	
Low	High	Low	3	1
		High	6	
	Low	Low	7	4
		High	8	

There are many benefits of an extended risk analysis process:

- Risks and controls are prioritised for attention using simple structures.
- The process generates a broader range of information and a wider set of indicators that decision-makers can use for making resource-allocation

decisions, for additional analysis, for treatment actions and for assurance activities.
- Very little additional effort is required in the risk analysis process.

The principles set out here will allow managers to make better use of their resources and satisfy the requirements of external reviewers and governance bodies.

7 References

Cox LA Jr. Evaluating and improving risk formulas for allocating limited budgets to expensive risk-reduction opportunities. Risk Analysis, 2012; 32(7):1244-1252.

Finger P, MacLeod A, Parkinson M and Purdy G. HB 158:2010, Delivering assurance based on ISO 31000:2009 Risk management – Principles and guidelines. Standards Australia, Sydney, NSW, The Institute of Internal Auditors Australia, Sydney, NSW, and the IIA Research Foundation, Altamonte Springs, FL.

ISO 31000:2009. Risk management – Principles and guidelines. International Organisation for Standardisation, Geneva. (Many national standards organisations also publish ISO 31000 in the form of a national standard for their own countries.)

8 Contact

If you would like further information about this topic please contact us. We will endeavour to reply within 48 hours.

Dr Dale F Cooper
Cooper@Broadleaf.com.au

Pauline Bosnich
Bosnich@Broadleaf.com.au

Dr Stephen Grey
Grey@Broadleaf.com.au

Grant Purdy
Purdy@Broadleaf.com.au

Geoff Raymond
Raymond@Broadleaf.com.au

Phil Walker
Walker@Broadleaf.com.au

Mike Wood
Wood@Broadleaf.co.nz

For further information visit www.Broadleaf.com.au

© 2014 Broadleaf Capital International Pty Ltd.
All rights reserved.