

# Broadleaf

**Creating value from uncertainty**

Broadleaf Capital International Pty Ltd

ABN 24 054 021 117

[www.Broadleaf.com.au](http://www.Broadleaf.com.au)

## Tutorial note:

# Controls 2: Introduction to control design

This tutorial is for line managers who are also risk owners, first to help them to think about where new or modified controls might be necessary, and then to select the most appropriate kinds of controls to address the risks for which they are responsible.

Version 1, 2018

## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Treatment options and control design</b>	<b>3</b>
<b>3</b>	<b>Conclusions</b>	<b>8</b>
<b>4</b>	<b>Contact</b>	<b>9</b>

## Tables

Table 1: Step-by-step process for control design	7
--	---

## Figures

Figure 1: Control design is part of risk treatment	4
Figure 2: Control design from risk analysis	5
Figure 3: Control design from gap analysis	6
Figure 4: Control design and control effectiveness	6

## 1 Introduction

This tutorial is for line managers who are also risk owners, first to help them to think about where new or modified controls might be necessary, and then to select the most appropriate kinds of controls to address the risks for which they are responsible.

A control is an 'enabler', something that enables a business objective to be achieved. For a risk owner, controls modify the consequences of a risk or the likelihood of those consequences, to greater certainty the organisation will achieve its objectives

The discussion in this tutorial provides general guidance; it is not tailored specifically to any particular risk. The concepts here can be applied to most situations and business activities, alongside existing or more risk-specific control standards.

## 2 Treatment options and control design

### Responsibilities

Risk owners (line managers) are responsible for designing and implementing controls for their risks.

Control owners are responsible for maintaining the effectiveness of the controls.

Assurance providers, such as internal audit at Line 3 of the three lines of assurance or specialist functions at Line 2, have skills that may assist in designing controls. This includes ensuring that the controls can be checked easily.

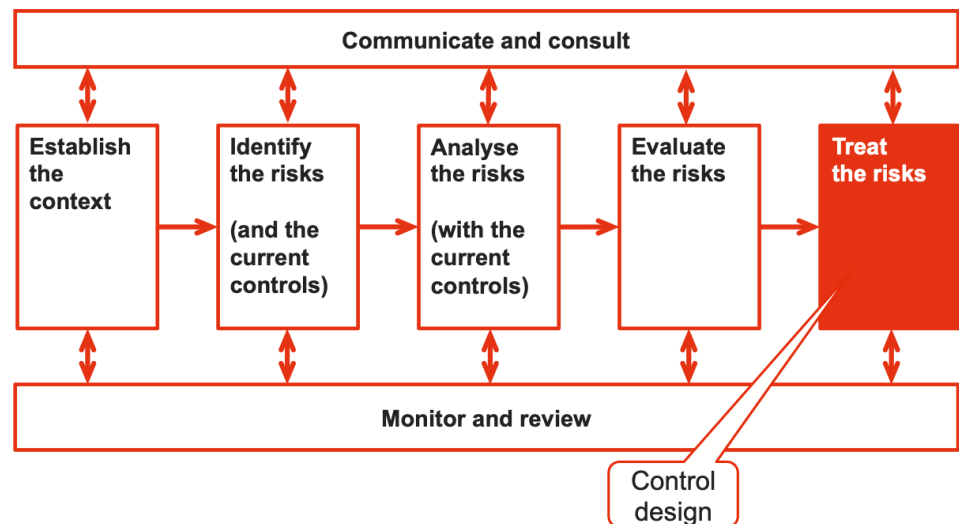
### Where does control design fit?

Control design is a central part of the risk treatment stage of the risk management process (Figure 1). Risk treatment involves developing options and selecting actions that will lead to the greatest net benefits for the organisation. When they are implemented, these actions will often result in

# Broadleaf

improved controls and greater control effectiveness. The concepts of control design discussed here assist in identifying feasible options that involve new or revised controls.

**Figure 1: Control design is part of risk treatment**



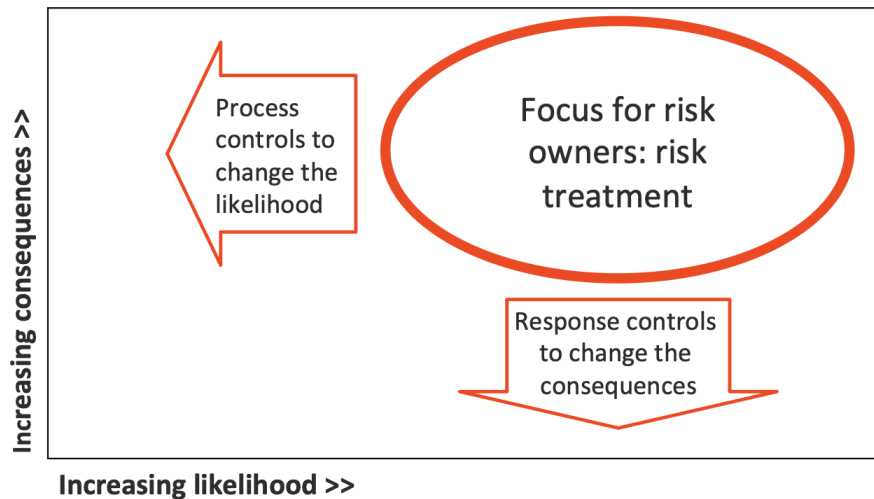
## Where are better controls needed?

There are several sources of guidance on where it would be useful to improve controls and what kinds of controls might be most appropriate. A risk analysis provides both an initial rating and an indication of the possible design intent for new controls (Figure 2).

- For risks with high likelihood, process or systems controls are likely to be most useful. These might be directed to increasing the reliability of a business process, better aligning the timing of business activities and increasing the diversity of controls to provide more ‘defence in depth’.
- For risks with high consequence, post-event responses are likely to be most useful, including contingency and disaster recovery planning, as well as insurance. Improving processes to detect abnormal events quickly and thus reduce the extent of adverse consequences may also be appropriate.
- Risks with both high potential consequences and a high likelihood of those consequences arising might require both types of control.

# Broadleaf

**Figure 2: Control design from risk analysis**

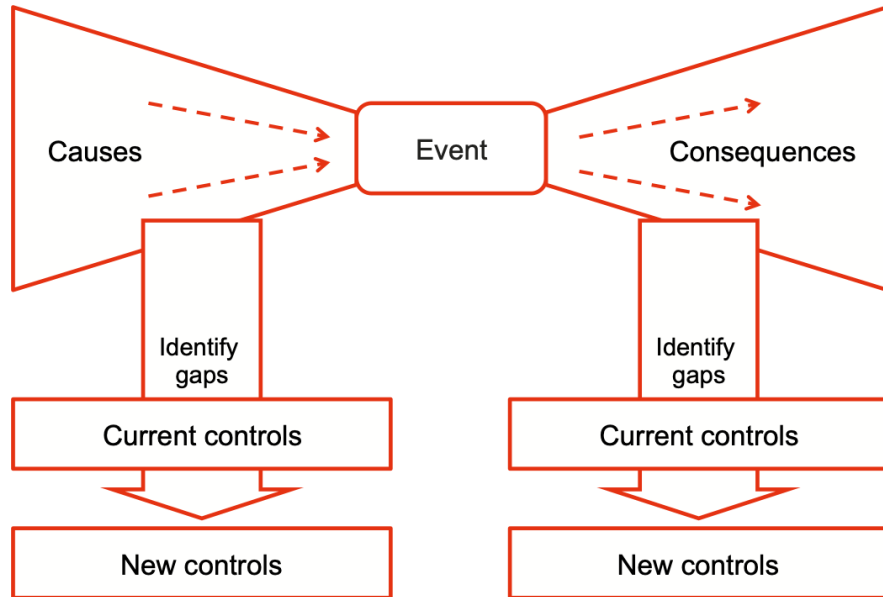


Going beyond the simple level of risk to more detailed analyses of the causes and consequences of the risk, and the existing controls, often provides a further guide to where new or improved controls might be sought and to their nature (Figure 3). Comparing causes and consequences with the existing controls that address them helps to identify gaps in the current controls.

- The most effective controls usually address causes, both internal and external, and both direct causes and indirect or root causes. The controls should match the causes, in extent and nature. This requires that the causes and their implications for business objectives be clearly understood, often in some detail. Techniques like bow tie analysis may be useful for this.
- For consequences, controls should provide appropriate responses to consequences being felt or barriers to the consequences developing, either to influence the consequences on business objectives directly or to detect changes quickly and provide triggers for contingency plans.

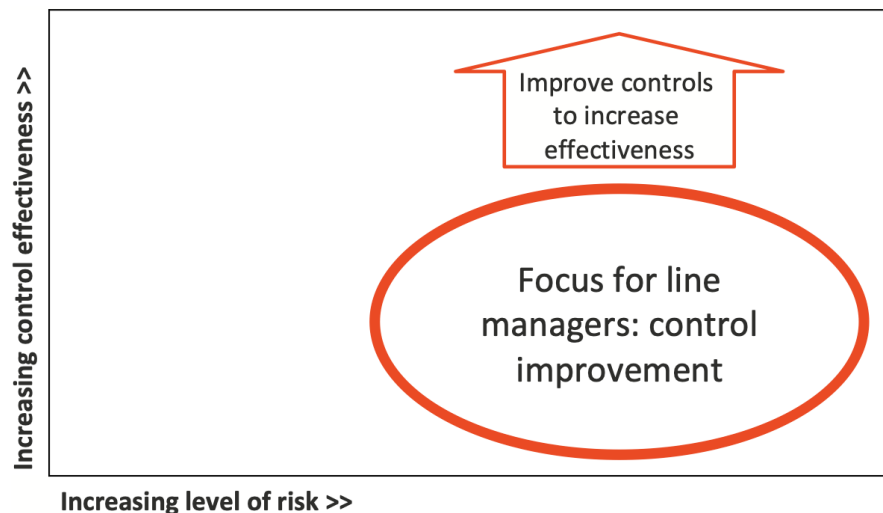
# Broadleaf

**Figure 3: Control design from gap analysis**



The risk analysis should provide an indication of the effectiveness of all the controls affecting a risk when taken as a whole. This is often in the form of an explicit rating of control effectiveness, a relative assessment of actual level of control that is currently present and effective for a particular risk, compared with that which is reasonably achievable by the organisation, as discussed in more detail in an earlier tutorial [here](#). Comparing control effectiveness with the level of risk (Figure 4) provides a way of prioritising the high risks – focus first on those high risks where the control effectiveness is low, as the analysis indicates that improvement is possible, particularly if control failure might be a contributor to the risk arising.

**Figure 4: Control design and control effectiveness**



## Designing better controls

For each risk, the controls as a whole should be:

- Fit for purpose, relevant and primarily address the root causes of the risk
- Appropriate, covering the full extent and scope of the risk and its consequences
- Efficient and cost-effective.

Ideally controls should be self-checking, so that if there is a failure they automatically generate an alert, or prevent an action from taking place. For example, a control sensor may generate a warning signal if the level of liquid in a tank is too high, and automatically shut down inlet pumps or prevent them from being turned on.

In most circumstances, actions to create new or revised controls will be implemented only if they generate a net benefit for the organisation, where the advantages and benefits outweigh the disadvantages and costs when considered as a whole. However, controls should conform to relevant standards or regulatory requirements, such as those imposed by workplace health and safety policy or legislation. In circumstances like this the net benefit criterion may not apply, and implementation must proceed, irrespective of net benefit, to satisfy compliance obligations.

Table 1 provides a summary guide to the six steps involved in detailed control design. The components in each of these steps have been discussed above.

**Table 1: Step-by-step process for control design**

Step	Topics
1. Identify causes, consequences and control gaps	Bow tie analysis showing causes, consequences and existing controls Sources of risk Control gaps
2. Define design intent	Extent and scope of controls that are needed to address related risks Ability of the control to be checked

# Broadleaf

3. Detailed design	Options to change the likelihood of the event and its consequences Options to change the consequences Options for addressing shared risks Control in depth
4. Evaluation and justification	Advantages and benefits compared with disadvantages and costs
5. Implementation	Task definition and purpose Task allocation and timing Communication, particularly between risk owners and control owners
6. Monitoring	Monitoring the timely and effective completion of improvement tasks Monitoring the continuing effectiveness of the control How and when monitoring will be conducted and recorded

## After a new control is implemented

When a new control has been implemented, or an existing control has been modified, any risk management information system should be updated. Ideally, the information system should contain a description of the control and what it is supposed to do (its design intent), as well as details of associated checking processes, whether monitoring, review or both:

- How it should be checked
- When it should be checked
- Who is responsible for making sure that checking takes place (the control owner).

The new or revised controls should be monitored under realistic operational conditions, and reviewed periodically, to confirm they are implemented well and working as intended.

## 3 Conclusions

Line managers who are also risk owners are responsible for control design. This is a core part of risk treatment.



Controls must be well designed and well implemented. The outcomes from a sound risk analysis process provide initial guidance. Assurance providers may play a useful advisory and facilitation role.

## 4 Contact

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

**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

**Mike Wood**

Wood@Broadleaf.co.nz

For further information visit [www.Broadleaf.com.au](http://www.Broadleaf.com.au)