Broadleaf

Creating value from uncertainty
Broadleaf Capital International Pty Ltd
ABN 24 054 021 117
www.Broadleaf.com.au

Tutorial note:
Controls 1: Introduction to control assurance

This tutorial introduces important concepts associated with controls and control assurance. The ideas and definitions provided here form a basis for more detailed material discussed in other related Broadleaf tutorials.

Version 2, 2018

Broadleaf

Contents

Tables

Figures

1 Introduction

This tutorial introduces important concepts associated with controls and control assurance. The ideas and definitions provided here form a basis for more detailed material discussed in other related Broadleaf tutorials (Figure 1):

1. This tutorial outlines the most important roles and responsibilities relating to controls and control assurance, describes important definitions and concepts, and outlines the main features of the three lines of assurance approach to assurance
2. The second tutorial (available here) concentrates on control design, an important part of risk treatment
3. The third tutorial (available here) discusses control review and describes how a manager can conduct a simple control self-assessment
4. The fourth tutorial describes approaches to monitoring controls
5. The fifth tutorial extends these concepts to more general planning of a control assurance program that might include an annual cycle of reviews.

Figure 1: Structure of the controls tutorials

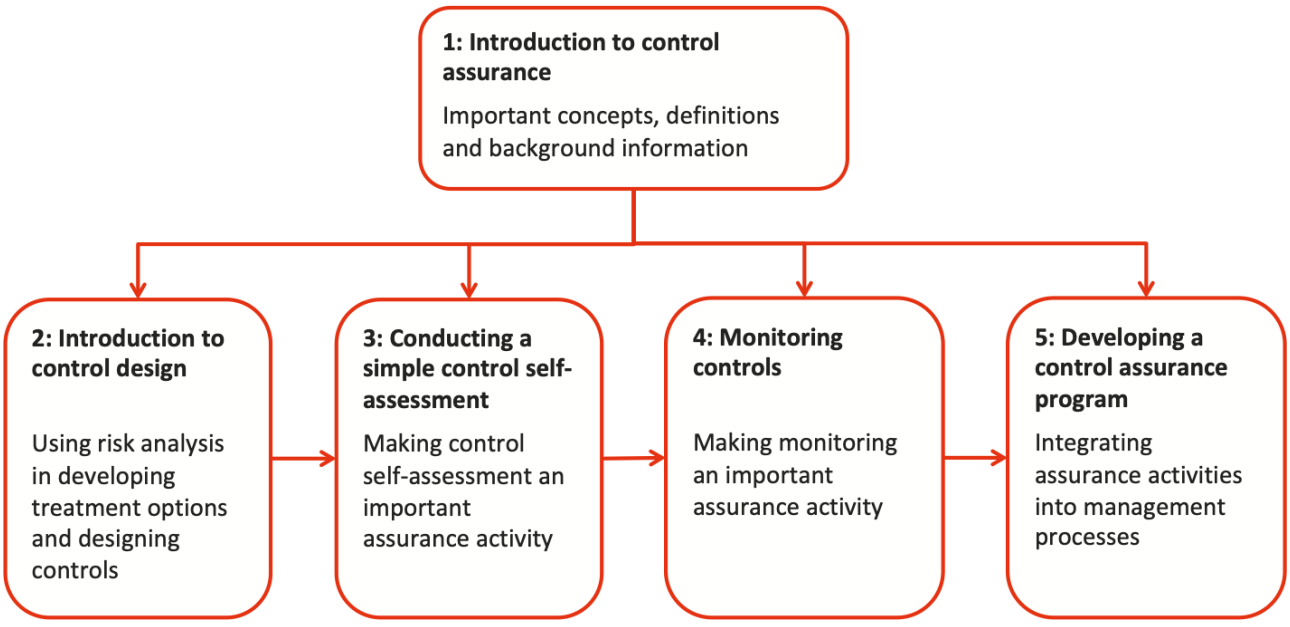
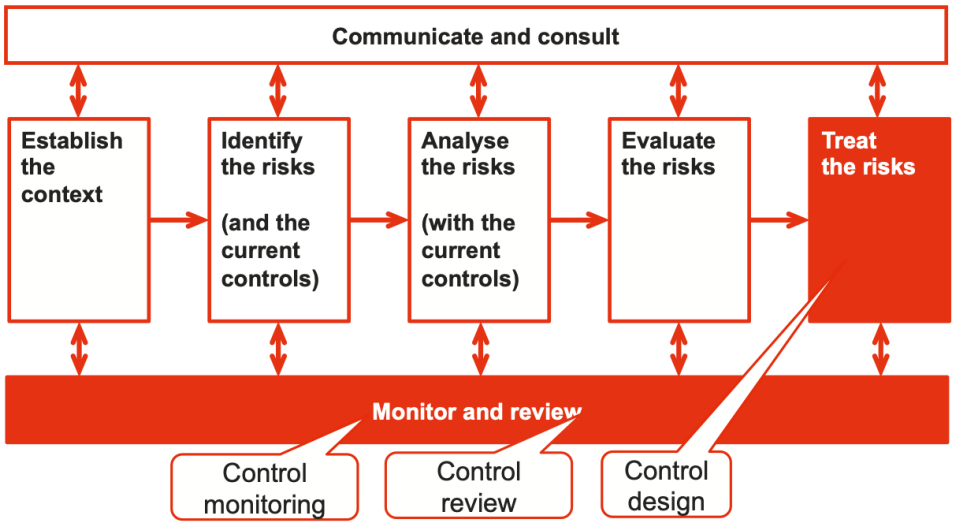


Figure 2 shows where the elements of control design, control monitoring and control review fit into the standard risk management process, specifically the risk treatment and the monitoring and review steps.

Figure 2: Where control design, monitoring and review fit



2 Roles and responsibilities

Risk owner

A risk owner is a person or entity with the accountability and authority to manage a risk, including determining controls.

Risk owners are usually line managers. They are responsible for designing and implementing controls for their risks.

Control owner

A control owner is accountable for implementing and maintaining the effectiveness of specific controls as recorded in a risk register, in a position description or in organisational policies and procedures.

Control owners may also be responsible for designing or modifying controls to improve their effectiveness.

One person might be a risk owner and a control owner for one or more controls related to that risk, but often the roles might be filled by separate individuals.

3 Concepts and definitions

Controls

A control is an 'enabler', something that helps an organisation achieve its business objectives. A control often arises from implementing a risk treatment action.

A control might take the form of a policy, procedure, device, system, communication or other action that acts to increase the certainty of achieving business objectives or to ensure compliance with the law.

A control may not always exert the intended or assumed modifying effect, so it is important to review its effectiveness critically.

Assurance

Assurance is a process that provides confidence that business objectives will be achieved with a tolerable level of residual risk. Checking the design and implementation of critical controls is an important component of assurance.

Adequacy

Risk management, control, and governance processes are considered adequate if management has planned and designed them in a manner that provides reasonable assurance that the organisation's objectives and goals will be achieved efficiently and economically (adapted from HB 158:2010).

Controls themselves, within the established control processes, are adequate if they have been planned and designed in a manner that provides reasonable assurance that the organisation's objectives will be achieved efficiently and economically, and that legal and contractual requirements are complied with.

Effectiveness

Risk management, control, and governance processes are effective if processes are operating in a manner that provides reasonable assurance that the organisation's objectives and goals will be achieved (adapted from HB 158:2010).

The effectiveness of controls describes whether the controls are operating as intended or not, and whether they will continue to operate when required.

Control effectiveness measure

Control effectiveness is a relative assessment of actual level of control that is currently present and effective, compared with that which is reasonably achievable by the organisation for a particular risk (adapted from HB 158:2010).

Control effectiveness is a relative measure, not an absolute one. It is relative to the level of control that is reasonably achievable by the organisation – even if the actual level of control is low, if that is all that is reasonably achievable then the controls can be 'fully effective'. This means that control effectiveness is really an indicator of management effectiveness.

Control effectiveness provides a means of prioritising risks for attention. If a risk has low control effectiveness, there is more that could be done and managers should be investigating and implementing improvement tasks. When a high risk has controls that are missing or weak, there should be risk treatment activities.

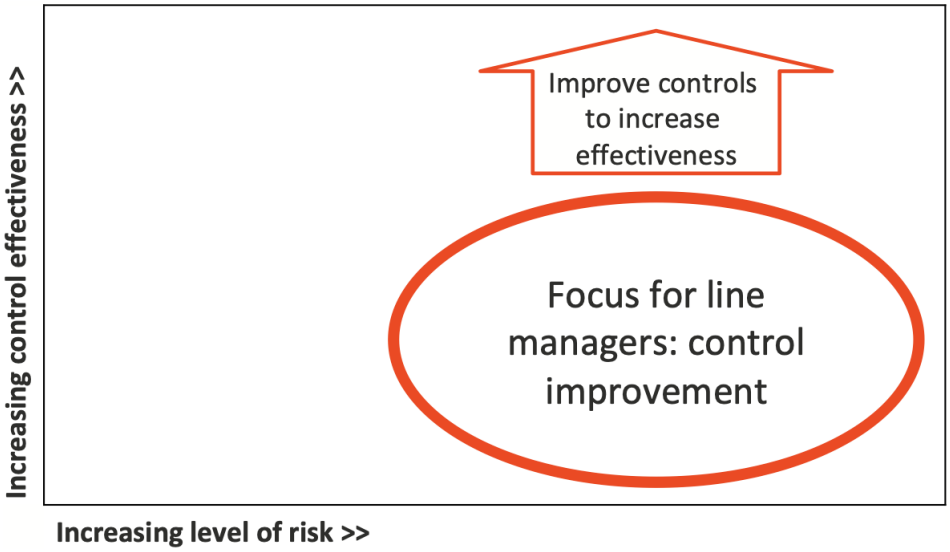
Table 1 shows a scale we often use for measuring control effectiveness, based on a similar scale in HB 158:2010.

Table 1: Control effectiveness scale

Rating	Guide
Fully effective	Controls are as good as realistically possible, both well conceived and implemented as well as they can be
Substantially effective	Controls are generally well designed and well implemented but some improvement is possible in their design or in how effectively they are implemented
Partially effective	Controls are well conceived but some are not implemented effectively or While the implementation is diligent, it is clear that better controls could be devised
Largely ineffective	There are significant gaps in the design or in the effective implementation of controls – much more could be done
None or totally ineffective	Virtually no credible control relative to what could be done

Comparing control effectiveness with the level of risk (Figure 3) provides a way of prioritising the high risks – focus attention for seeking better controls 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 3: Control design and control effectiveness



Potential exposure

Potential exposure is the total plausible maximum impact on the organisation arising from a risk without regard to controls (adapted from HB 158:2010).

Potential exposure provides a simple, reliable and realistic means to focus audit and assurance activities. It is more useful than the ambiguous concept of 'inherent risk' as a means to prioritise assurance activity.

Potential exposure is sometimes referred to as potential maximum loss or maximum potential consequences. It is often estimated using the same consequence criteria scales that the organisation uses for risk analysis, which allow all the organisation's objectives to be included in its assessment, not only those expressed in financial terms. In some circumstances narrower measures are used instead, defined in terms of the maximum financial loss or the maximum number of fatalities that might arise.

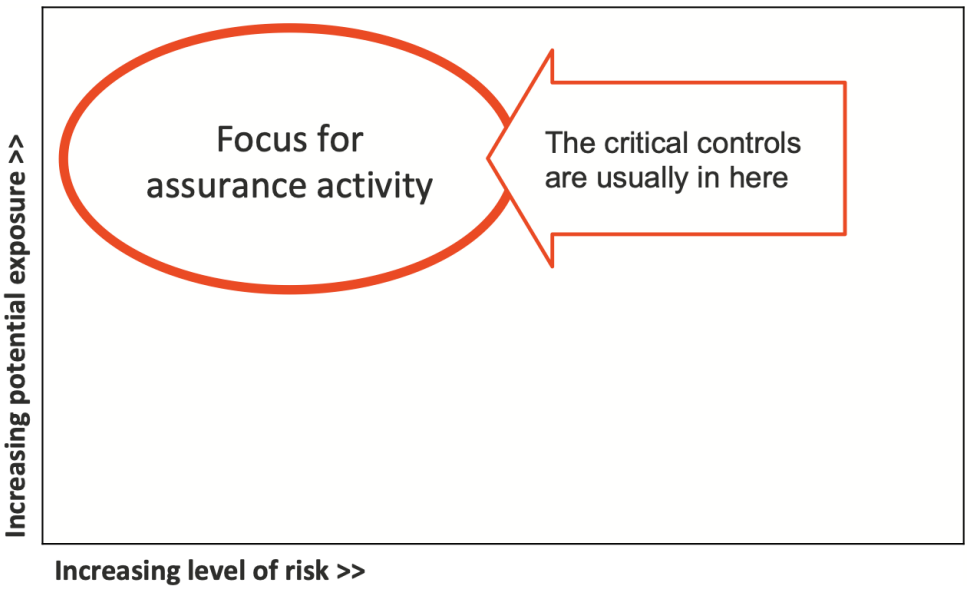
Critical controls

Critical controls are those whose effectiveness contributes materially to the achievement of the organisation's strategic or business objectives, or that are required for policy, contractual or regulatory compliance. If these controls fail to operate as planned, the organisation will be exposed to the possibility of serious undesirable consequences, so it is important for control owners to test the controls periodically to ensure they work.

Critical controls are often associated with risks where the consequences might be high or very high if the controls were to fail, with a potential exposure or maximum possible loss, described earlier. The top-left region of the diagram in Figure 4 shows the combination of risk level and potential exposure where risks associated with critical controls will generally fall.

At first sight, it might seem unusual to focus on risks falling at the lower end of the risk scale, at the left hand end of the horizontal axis. However, in this region where the levels of risk are rated low with the controls in place, the loss if the controls were to fail would be high. A low level of risk can lead to complacency, but the point of control assurance is to protect against the potential consequences, not necessarily to reduce further the level of risk. (The top-right region in Figure 4 is also important, but this is usually a focus for risk managers who are trying to improve the relevant controls and will attract attention because it contains risks with high ratings.)

Figure 4: Critical controls



4 Three lines of assurance

Overview

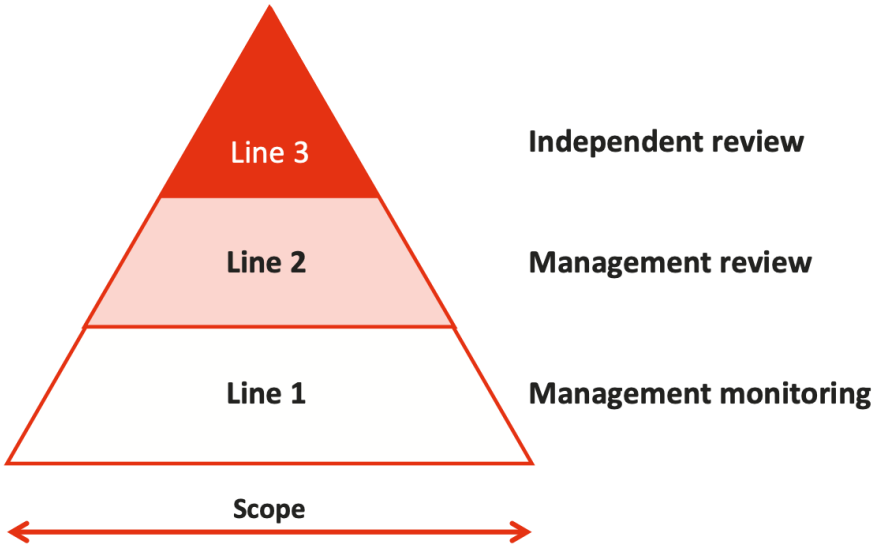
Assurance is a process that provides confidence that objectives will be achieved within an acceptable level of risk. It involves checking the critical controls.

Assurance normally includes all three of the following elements:

1. Specific day-to-day control monitoring, preferably built into systems and procedures such as routine oversight and status checks, described in a separate tutorial
2. Periodic reviews by control owners using control self-assessment, described in a separate tutorial here
3. Occasional verification by assurance providers or auditors who are independent of line managers.

Assurance is often visualised in terms of the three lines of assurance shown in Figure 5 that address the three points noted above.

Figure 5: Three lines of assurance



Line 1: management monitoring

Line 1 includes all routine controls and process checks, often embedded into procedures and methods of working. Managers at Line 1 are responsible for maintaining effective internal controls and for executing risk and control

procedures on a day-to-day basis. They may conduct control self-assessments as part of their responsibilities.

The scope of Line 1 assurance extends across the whole organisation and its activities.

Line 2: management review

Line 2 includes checks on processes and systems, often using control self-assessment, driven by the risk profile of the business area and the manager's span of control. Managers at Line 2 set and monitor policies, systems and governance processes that review how risk and compliance is undertaken across the business.

Sometimes Line 2 oversight is provided by specialist functions that exercise oversight over particular areas such as health and safety, environmental management, asset integrity, technical engineering, project management or financial middle office functions. Such specialist Line 2 functions are often largely independent of operational managers.

The business or organisational scope for Line 2 is more limited than for Line 1, and often focused on higher-level processes within a business area or function.

Line 3: independent review

Line 3 provides a level of independent assurance that risk management and internal control frameworks are working as intended. Line 3 assurance is usually provided by internal audit and external audit, sometimes augmented by special-purpose independent audits.

Independent audits tend to have a very specific focus, and they are rarely able to cover the full scope of business activities.

5 Monitoring and review

Overview

'Monitor and review' is one of the most important steps in risk management, and central to providing assurance. The activities conducted as part of this step help to ensure the risk management process is dynamic and responsive to change, rather than generating a historical 'snapshot' of the organisation at

some previous time. They also provide the basis for fundamental assurance of controls for line managers, the Executive and the Board.

Monitor and review is most successful when it is integrated into key decision-making processes and appropriate resources are assigned. This is discussed in more detail in a separate tutorial.

Monitor

Monitoring usually involves continuous or close-to-continuous surveillance of activities or indicators of change. It is conducted by line managers or supervisors at Line 1 of the three lines of assurance, or by review functions at Line 2. For example,

- Personnel in production control centres and operations control rooms monitor a wide range of indicators and alerts to enable them to identify undesired events or trends that may be precursors to undesired events, and then to initiate appropriate responses (Line 1)
- Specialist functions at Line 2, such as environmental management teams or maintenance teams, may monitor indicators less frequently, but with a similar purpose, to identify undesired events or trends that may be precursors to undesired events, and then to initiate appropriate responses.

Monitoring is discussed in more detail in a separate tutorial.

Review

Reviewing is a periodic checking activity to examine processes and outcomes from time-to-time, to help to identify areas where improvements might usefully be made. Independent auditors at Line 3 and oversight functions at Line 2 should conduct reviews, particularly of critical controls. Managers at Line 1 should conduct reviews of critical areas where a more detailed examination of processes may be required than routine monitoring can provide.

Control self-assessment is an important review tool for managers at Line 1 and Line 2. Reviewing in the form of control self-assessment is discussed in more detail in a separate tutorial here.

6 Reference

Finger, Pamela, Andrew MacLeod, Michael Parkinson and Grant Purdy (2010) *HB 158-2010 Delivering assurance based on ISO 31000:2009 Risk management – Principles and guidelines*. Standards Australia, The IIA Research Foundation and The Institute of Internal Auditors Australia.

7 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