

# 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 5: Developing an assurance program

This tutorial is for directors and managers who need assurance that critical controls are in place and working, and that they will work in the future if they are needed. To be effective, assurance must be a planned and deliberate activity. This tutorial discusses how to develop an assurance plan that is appropriate for your organisation.

Version 1, 2019

# Broadleaf

## Contents

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>Introduction</b>  | <b>3</b> |
| <b>2</b> | <b>Responsibilities</b>                                      | <b>3</b> |
| <b>3</b> | <b>Planning and integration of routine assurance reviews</b> | <b>3</b> |
| <b>4</b> | <b>Conclusions</b>   | <b>7</b> |
| <b>5</b> | <b>Contact</b>   | <b>7</b> |

## Tables

|   |   |
|---|---|
| Table 1: Planning control assurance for a line manager    | 4 |
| Table 2: High-level focus for an Audit and Risk Committee | 6 |

## Figures

|                                    |   |
|------------------------------------|---|
| Figure 1: Business assurance cycle | 5 |
|------------------------------------|---|

## 1 Introduction

This tutorial is for directors and managers who need assurance that critical controls are in place and working, and that they will work in the future if they are needed. In particular, the approach described here will be useful for:

- Risk owners, for the key controls associated with their risks
- Control owners, for the controls for which they are accountable
- Managers who oversee parts of the business where risks may arise and who must either conduct, or review the conduct of, assurance activities
- Directors and members of Board Audit and Risk Committees who must oversee and authorise the planning and implementation of assurance activities, including internal audit plans.

## 2 Responsibilities

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

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

Risk owners, control owners and managers who oversee parts of the business where risks may arise may all need to conduct control self-assessments, the subject of a separate Broadleaf tutorial.

Directors and members of Board Audit and Risk Committees must oversee assurance activities, including appointing internal auditors and authorising the planning and implementation of internal audits. They need to be confident that assurance plans are in place throughout the organisation, and that internal and external audit plans are appropriate.

## 3 Planning and integration of routine assurance reviews

Control self-assessment will not occur unless it is planned and the plan is implemented. Integrating it and embedding it into normal business, while ensuring that it remains a distinct activity and is not subsumed into other processes to the extent that it might lose focus, is the most successful strategy.

# Broadleaf

Examples of where assurance activities could be integrated include:

- Managers' walk-around
- Toolbox talks
- Standing agenda items on management meetings
- After the investigation of a success or a failure.

Checking 'everything at once' is rarely a useful or practical approach. If the process is too time consuming, there is a danger that personnel will find ways to give it lower priority, make excuses to avoid it or allow the quality to decrease. It is better to plan a cycle of assurance reviews over a period, so that by the end of the period all the important controls have been reviewed at least once. There are several ways a manager might disaggregate her areas of responsibility to identify suitable controls or groups of controls for review (Table 1).

**Table 1: Planning control assurance for a line manager**

| Basis                   | Description  |
|-------------------------|--|
| One control at a time   | Use the information system to prompt when the control should be reviewed on a regular cycle, say quarterly, every six months or annually, according to its importance  |
| Physical areas          | This works best where processes are defined and located in specific areas (e.g. sites, work areas, offices)<br><br>Aim to cover all physical areas under the manager's direct control within a periodic assurance cycle (e.g. annual or monthly) |
| Functions or activities | Start with a comprehensive process map of functions or processes within the manager's span of responsibility or direct control   |
| Sources of risk         | Plan and schedule assurance reviews according sources of risk<br><br>This is more suitable for generalised reviews at a business unit level rather than for an individual manager  |

# Broadleaf

Many of the reviews undertaken by a line manager are likely to involve control self-assessments. The way to conduct simple control self-assessments was described in an earlier [tutorial note](#).

There are several factors to take into account when developing the assurance plan:

- The plan should be comprehensive, so every important control is checked at least once across the cycle
- The plan should allocate activities throughout the year, to avoid a large and unsustainable workload associated with a single completion date
- The plan should be aligned with the corporate calendar, so that assurance activities align with other corporate obligations; for example, assurance associated with financial matters might be aligned with financial reporting requirements, tax matters might be addressed before tax returns are submitted and so on
- Some controls, such as those associated with employee safety, might be addressed more than once across the cycle because they are particularly important
- The plan should be adjusted according to what is included in assurance plans developed by other Line 2 functions, and with internal and external audit plans, to avoid excessive duplication or overlap.

Figure 1 shows an example of an annual assurance cycle for an organisation, with two focus areas each month.

**Figure 1: Business assurance cycle**



# Broadleaf

Similar planning cycles should be developed for business units and divisions, to ensure that risks and controls that are relevant to the unit are examined regularly. Feedback from such programmes also allows risk registers to be kept up to date with little extra effort, rather than being historical snapshots of past circumstances.

The cycle is not intended to be so rigid that it constrains managers from making sensible decisions about the conduct of assurance activities. For example, reviews might be conducted out of sequence if circumstances change, or if a significant control failure occurs or is suspected, whether in the organisation or in the wider business sector in which it operates.

Table 2 shows a similar stewardship cycle that might form part of the agenda for a Board Audit and Risk Committee. Again, timings would be set according to corporate or regulatory calendars. Table 2 only shows when the major discussions are scheduled; details associated with many individual topics would be addressed routinely in every meeting, with the annual discussion focusing on an overview and wider systemic matters.

**Table 2: High-level focus for an Audit and Risk Committee**

| Month    | Major topics   |
|----------|--|
| February | External Audit Plan<br>Insurance   |
| April    | Risk management: major status review; ERM framework; ERM Plan; risk management in major projects; emerging risks; implementation of risk treatment actions                           |
| June     | Audit and assurance: major status review; Internal Audit Charter and Policy; Internal Audit Manual; Internal Audit Plan; implementation of assurance actions<br>Financial statements |
| August   | Financial statements   |
| October  | Business security: business continuity management; incident response plans; physical security; information security  |

| Month    | Major topics   |
|----------|--|
| December | Compliance matters: ethics, fraud and corruption; legislative compliance; delegations of authority; policies and procedures<br>Audit and Risk Committee Charter<br>Audit and Risk Committee performance review |

The requirement to plan assurance activities remains essentially the same, whether those activities are to be undertaken by management or independently by an internal or external audit function. An assurance plan for management would be part of the broad 'controls environment' an auditor would take into account when preparing an internal or external audit plan.

## 4 Conclusions

Assurance must be a planned and deliberate activity. Ideally, it should be integrated into routine business activities. A planned assurance cycle is strongly recommended.

## 5 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