Good Governance Guide

Risk management policy

Governance Institute of Australia

Not-for-profit sector

It is considered **good governance** that a not-for-profit organisation have in place a risk management policy, which is to be subject, where relevant, to the terms of reference of the board audit and/or risk management.

The policy could include the following:

- a mission statement on risk, including a definition of risk such as 'anything that hinders the sustainable achievement of objectives and results, including the failure to exploit opportunities'
- the purpose of the policy, which is to formalise and communicate the organisation's approach to the management of risk
- the scope of the policy
- the organisation's risk tolerance level
- the roles and responsibilities of :
  - the board
  - the board audit and/or risk management committee
  - management
  - the risk manager or other officer who assumes this duty
- other risk activities of the various groups within the organisation
- external audit responsibility
- the risk assessment, measuring and reporting process
- the risk identification and profile continuous monitoring.

After approval by the board, the policy should be signed and dated by the chief executive and circulated as appropriate within the organisation.

The policy should be reviewed on a regular basis, for example, a year after the first implementation, and then every three years.

Refer to Good Governance Guide: *Risk management overview* for more information.