

AGENCY POLICY:**RISK MANAGEMENT**

Policy number: 14.1/0

Date of Issue: April 2014

Contact: Business Assurance Manager

Phone: (02) 8536 0822

 form
  filing
  copy

1. Purpose

The overall goal of this policy is to reduce CatholicCare's risk to an acceptable level to support CatholicCare's strategic objectives and appetite for risk and ability to realise opportunities.

The Board has delegated day-to-day risk management to the Executive Leadership Team with Board oversight via risk reporting to the Board and Executive update.

This policy is part of the Risk Management Framework that establishes a consistent approach to identifying, managing and monitoring risk across CatholicCare and underpins the development of a robust risk culture within the organisation.

CatholicCare's risk management policy should be read in conjunction with the following separate documents:

- Risk Management Framework
- Risk Management Procedure
- Risk Appetite Statement
- Audit and Risk Committee Terms of Reference

2. Risk Management Policy

Risk is the effect of uncertainty on objectives, where an effect is a positive and/or negative deviation from the expected. It is the chance of something happening that will have an impact on objectives. Risk management is the culture, processes and structures that direct and control an organisation with regard to risk.

Risk management involves the systematic application of management policies, practices and procedures to the task of identifying, analysing, assessing, treating, monitoring and communicating risk i.e. "what could happen" and "what should we do about it". It

The Board's policy is to maintain a sound framework of risk oversight, risk management and internal control.

CatholicCare's risk management framework is designed to:

- identify, analyse, assess, treat and monitor risk
- identify material changes to the organisation's risk profile
- articulate CatholicCare's risk appetite.

CatholicCare recognises that the effective management of risks is a vital element in fulfilling its mission and values, meeting strategic goals and objectives, mitigating



potential loss, maximising opportunities and meeting corporate governance requirements.

2.1 To ensure risk is effectively identified, analysed, evaluated, mitigated and monitored throughout the organisation, CatholicCare will:

- 2.1.1 Maintain a formal and ongoing risk management process.
- 2.1.2 Identify risk management as a core responsibility of all management that will be overseen by the Executive Leadership Team and ultimately the Board.
- 2.1.3 Document roles and responsibilities – see Risk Framework.
- 2.1.4 Fully integrate risk management into the annual business planning process.
- 2.1.5 Ensure risk is on the Board agenda via Board Audit & Risk Committee reporting.
- 2.1.6 Ensure that any major submissions to the Board include commentary on the identified risks.
- 2.1.7 Develop and maintain a central register of strategic risks, appropriate mitigation strategies and actions.
- 2.1.8 Ensure statutory and regulatory compliance with legal, accreditation, licensing and contractual obligations through a suitably resourced Business Assurance function.
- 2.1.9 Establish an annual Board and Executive - Risk Management Workshop, the purpose of which is to ensure that CatholicCare establishes and maintains an appropriate risk management process including:
 - Identifying and assessing the risks to CatholicCare's vision, mission, values and objectives.
 - Assigning and implementing risk mitigation or improvement strategies including business continuity planning.
 - Follow-up, review, testing and reporting risk management and business continuity to the Executive Leadership and the Audit and Risk Committee of the Board.

3. Risk Management Framework.

There are three major elements within CatholicCare's Risk Management Framework that provide the operational framework that spans the organisation and recognises the Board's role in oversight:

- The Risk Management Process
- Emergency Response and
- Business Continuity.

These structures are illustrated within the CatholicCare Risk Management Framework and provide direction on how risks and major issues will be dealt with in the event of business continuity being affected.

4. Definitions of Risks



The Risk Register (see section 7) maintained as part of the organisations Enterprise Risk Management system incorporates definitions of each risk identified by CatholicCare under the Key Risk Areas of:

- Strategic
- Financial
- Operational
- Reputational

5. Procedure

The detailed processes involved in the identification of risks and the design of effective risk management plans are contained in the Agency Procedure: Risk Management.

6. Annual Board and Executive Risk Management Workshop

An annual Risk Management Workshop will be conducted and coordinated by the Chief Financial Officer. Participants in the workshop will include senior representation from each Directorate/business unit.

The Risk Management Workshop will: identify and quantify any new or emerging strategic risks that need to be considered within the preparation of business plans; review existing risk and business continuity plans and review progress on identified strategies and actions.

Risks identified and quantified from the Risk Management Workshop will be assigned to senior managers who will be responsible for implementing and monitoring the risk mitigation process in their areas of responsibility.

7. Risk register

Risks are maintained within a central risk register. The risk register incorporates definitions of each risk identified by CatholicCare under the Key Risk Areas of:

- Strategic
- Financial
- Operational
- Reputational

All risks will include a risk rating, designated Risk Owners, mitigation strategies/controls and time lines where appropriate.

Risks will be assessed in terms of:

- Inherent likelihood, consequence and rating (that is the risk if we do nothing).
- Residual likelihood, consequence and rating (the risk after the mitigation strategies and actions are implemented).

Ongoing mitigation strategies/controls will be identified and assigned to Control Owners.

For key risks, specific actions may be required to manage risk mitigation strategies/controls and actions will be reported through the annual business plans provided by the Executive Leadership Team.

The CatholicCare Risk Register, will be updated as new risk information is identified.

8. Assigning Responsibility

Board has overall responsibility for risk. Roles and responsibilities are outlined in the Risk Framework. The CEO has ultimate Executive responsibility and this may be delegated to an appropriate senior manager.

9. Review

This policy shall be reviewed at least annually by the CEO or as directed by the Board Audit and Risk Committee.

10. References

- AS/NZS ISO 31000 – Risk Management
- AS/NZS 5050:2010 – Business Continuity
- Agency Procedure: Risk Management

