CatholicCare
DIOCESE OF BROKEN BAY

Agency Risk Management Framework

Version: 1.0
Approved: 7 February 2024
Review due: February 2027
Document ID: 10077-012

Contents

Purpose 3
Scope 3
Overview 3
- Approach to Managing Risk 4
- Responsibilities 4
- Three lines model – Managing Risk and Coordinated Assurance 6
- Governance 7
- Risk Assessment and Management Process 8
- Shared Risk - Evaluation and Assessment 9
- Escalation 10
- Monitoring and Review 11
- Key Risk Register Reporting to Advisory Council 11
- Risk Closure 11
- Risk Culture 11

Related documents 12
Glossary 12
Sign off and review 14
Revision history 14

Purpose

The purpose of the Risk Management Framework is to articulate the organisational arrangements for designing, monitoring, reviewing and continually improving risk management practices throughout CatholicCare Diocese of Broken Bay (CatholicCare). It describes risk management elements and tools used at CatholicCare to achieve Risk Management Policy objectives and to integrate risk management into all CatholicCare activities.

Scope

This Risk Management Framework applies to all staff, contractors, volunteers, Advisory Council and Committee members, and work placement students of CatholicCare. CatholicCare acknowledges that as an agency of the Diocese we are required to manage and report risk on behalf of and to the Bishop.

Overview

This Risk Management Framework should be read in conjunction with the *Risk Management Policy*, the *Risk Management Practice Guidelines* and the *Risk Appetite Statement*.

The Framework articulates the organisational arrangements that form the basis of risk management across CatholicCare.

The Policy and Practice Guidelines establish the procedures and practices that staff are required to follow to implement the Framework and support CatholicCare to manage risk.

The Risk Appetite Statement articulates the predetermined level of risk that CatholicCare is prepared to accept as we undertake the various activities that support our strategic directions. CatholicCare has different risk appetite tolerances for different categories of risk.

Our framework includes the following elements:



Approach to Managing Risk

CatholicCare's approach to risk management must be **timely, appropriately structured, monitorable**, and consistent with our Risk Appetite Statement. Our processes and practices:

- Explicitly address "uncertainty" in relation to achieving significant objectives and priorities, with a view to reducing variability in potential outcomes.
- Are specific and context driven in identification of uncertainty.
- Recognise the impact of people, culture, and environmental factors on objectives.
- Are consistent with our governance and compliance requirements.
- Ensure decisions are as transparent and inclusive as possible.
- Are supported by best available information and record keeping practice.
- Help protect and leverage our people and assets to further our mission.
- Are responsive to change and improvement.

Responsibilities

The Executive Director of CatholicCare is responsible for:

- Managing overall agency risk.
- Ensuring that CatholicCare has a robust Risk Management System, including Risk Registers developed in consultation with the Senior Leadership Team.

- Setting the cultural tone and monitoring the effectiveness of risk management activities across CatholicCare.
- Reporting to the Advisory Council of CatholicCare on risk (including through the Finance & Risk Sub-Committee).
- Integrating risk management into strategic, financial, and operational planning for the agency.

The Advisory Council of CatholicCare is responsible for:

- Providing advice to the Executive Director and to the Bishop in relation to key business risks, risk management practice and alignment of values.
- Supporting the development and implementation of CatholicCare's Strategic Directions, with a risk management lens.
- Identifying key KPIs for monitoring and reporting of risk.

The Senior Leadership Team are responsible for:

- Identifying and managing risk in their relevant business area.
- Maintaining the Operational Risk Register.
- Participating in the monitoring and review of the Key Business Risk Register.
- Overseeing the risk management activities of their direct reports and teams.

Executive Manager Quality, Safeguarding, Risk and Compliance has particular responsibilities including:

- Coordinating risk reporting to relevant CatholicCare and Diocesan committees.
- Arranging risk management training for CatholicCare managers and staff.
- Coordinating Senior Leadership Team reviews of the Key Business Risk Register.
- Conducting trend analysis of incidents and complaints.
- Reviewing serious and critical incidents.

Managers (at all levels) and Coordinators are responsible for:

- Integrating risk management into planning and operational processes.
- Identifying and managing risks across their operational portfolio.
- Consulting with staff and other stakeholders (including clients, families, funders, and other external stakeholders) to ensure potential risks are identified, analysed, evaluated, and then eliminated, reduced, or controlled.
- Ensuring staff and volunteers have access to appropriate training, resources, and support to effectively manage operational risks within their scope.

All staff:

All staff are responsible and accountable for assisting in the identification and management of risks in their workplace on an ongoing daily basis.

Three lines model – Managing Risk and Coordinated Assurance

The “three lines model” is relied upon for allocating responsibility and accountability for risk management across three functions.

In the CatholicCare context, CatholicCare service centres are the 1st-line and will receive support from more centralised 2nd-line CatholicCare teams in managing risk. The 3rd-line provides assurance over the 1st-line and 2nd-line work.

Governance			
3rd Line Independent, objective assurance	Independent assurance by evaluating and giving an opinion of the adequacy and effectiveness of risk management and controls.	Assurance from external audit and oversight on specific risk Internal Audit	External Assurance Providers
2nd Line Oversees/challenges Risk related issues	Reviews and challenges 1st line regarding the effectiveness of controls through oversight of processes and risks Semi-independent reviews, inspections, investigations.	Senior Leadership Team Diocesan Governance & Risk Executive (DGRE) WHS Committees Quality, Safeguarding, Risk and Compliance Team	
1st Line Owns, manages day-to-day risk in service delivery	Day-to-day risk management decisions by staff. Managers, Coordinators & Supervisors who implement and action controls and monitor them to ensure they are effective.	Management Controls Internal Control Measures (Policies, procedures, systems, frameworks, structures, and people)	

1st-Line: Owns and Manages risk decisions for day-to-day operations

Most staff have a 1st-Line responsibility. The 1st-Line have the **primary responsibility to own the risks associated with day-to-day operational activities**. Other accountabilities assumed by the 1st-Line include the design, operation, and implementation of controls over processes, monitoring, and reporting.

All 1st-line workers *identify* risks, *assess*, *prioritise,* and effectively *manage* risk within their area of responsibility.

2nd-Line : Oversees

The 2nd-Line have the **primary responsibility to advise and challenge the 1st-line regarding risks and controls**. The 2nd-line does this by undertaking compliance and oversight by designing process frameworks, policies, procedures, tools, and techniques as well as semi-independent reviews, inspections, and investigations. In our context the 2nd-line is likely to include:

- Executive Director
- Executive Manager Quality, Safeguarding, Risk and Compliance
- Senior Leadership Team
- Centralised support teams: People & Culture, Information, Work Health & Safety, Communications & Engagement, Quality, Safeguarding, Risk & Compliance. Leaders at the service centre etc.

All 2nd-Line workers *identify* risks, *assess*, *prioritise,* and effectively *manage* risk within their specific 2nd-Line area of responsibility.

2nd-Line workers support 1st-Line workers to manage risk by providing guidance and support.

3rd-Line: Provides Independent Assurance

The 3rd-Line function provides objective and independent assurance to the Executive Director. The **3rd-Line's key responsibility is to assess whether the 1st and 2nd Line functions are operating effectively**.

CatholicCare currently receives independent assurance regarding annual financial accounts and are the subject of other external oversight and compliance due to the nature of the services we provide (e.g., Office of Children Guardian, NDIS Commission) and undergoes several external audits to maintain accreditation.

Governance

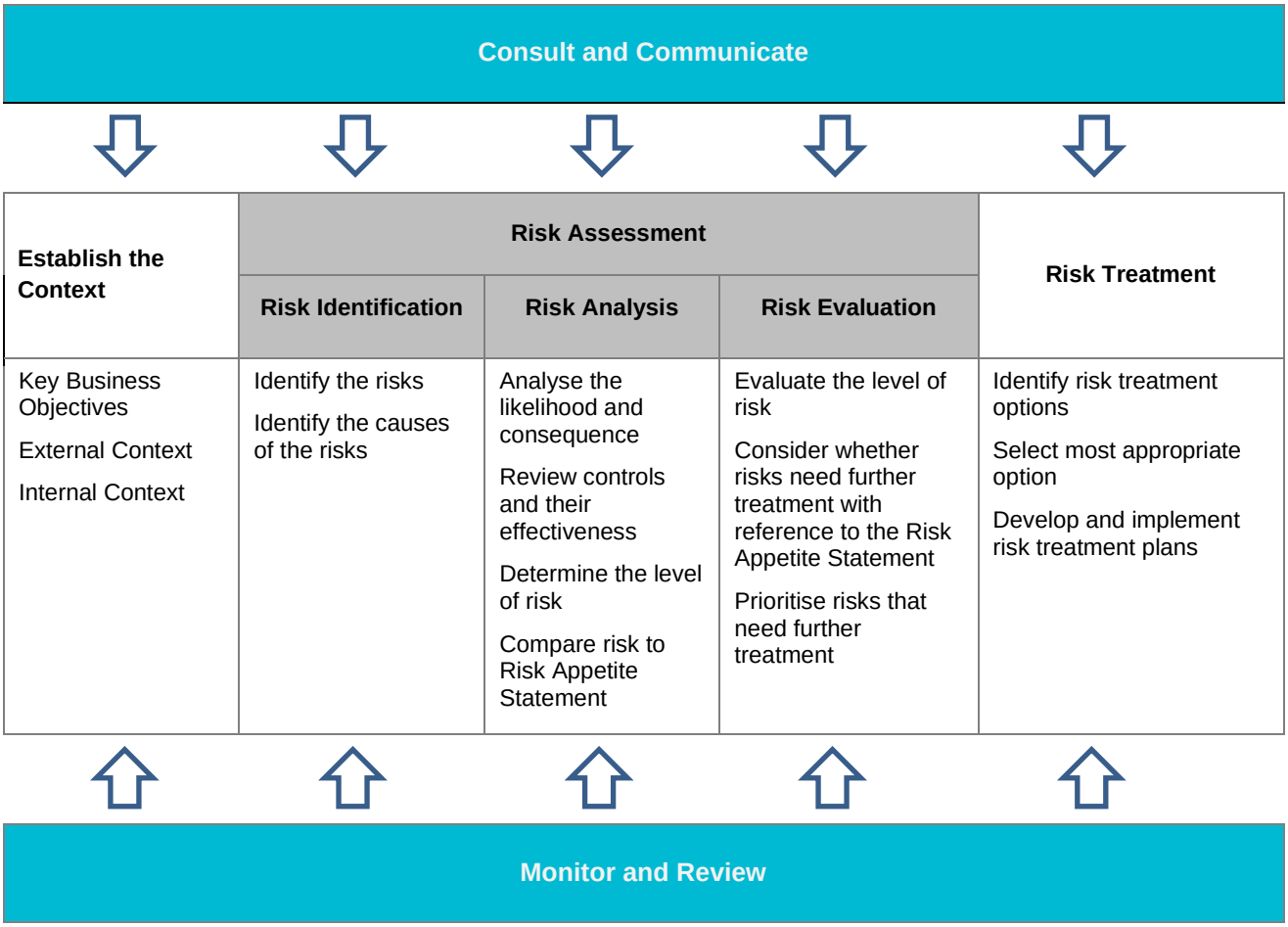
As delegated by the Trustees, our Executive Director in his/her governing capacity, sits over the three lines. The governance function is supported by:

- CatholicCare Advisory Council
- CatholicCare Finance Audit & Risk Sub-Committee
- CatholicCare Clinical & Care Governance Sub-Committee
- The Diocesan Governance and Risk Executive Committee

Risk Assessment and Management Process

Risk assessment is the overall process of risk identification, analysis, and risk evaluation. The risk management process is applied to each risk, and the main steps in the management process are depicted in the diagram below. The 1st-Line and 2nd-Line as well as other responsible and accountable management should apply existing policies, procedures and practices when establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risks.

The risk management process is the 'how to' element of the framework and is defined by the Australian and New Zealand Standard AS/NZS ISO 31000:2018 Risk Management as "the systematic application of management policies, procedures and practices to the task of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk".



This is a step-by-step iterative process and needs to be an integral part of management and decision making.

Below is a summary of the steps required to assess and manage risk. The CatholicCare Risk Management Policy contains more detailed information on each of these steps.

Steps	Action
1. Communicate and Consult	This step requires sound communication between the Risk Owner and staff or other stakeholders about potential risks and how those risks might be managed. This step is important because it brings different areas of expertise together. It also builds a sense of inclusiveness and ownership as risks are managed.
2. Establish the Scope, Context and Criteria	This step customises the risk management process to the context of the environment in which the risk exists. It also enables effective risk assessment and appropriate risk treatment. This is done by defining the scope and understanding the external and internal context in the environment in which risk is being assessed and managed.
3. Risk Assessment	This step is necessary before the risk can be treated, and requires the risk to be identified, analysed and evaluated. a. Identify Risk There are some common techniques used to identify risk, which are listed in the Risk Management Policy, but can be as simple as a meeting of the Risk Owner, staff and any other stakeholders that might assist in identifying risk. b. Analyse Risk Once Material Risks are identified and categorised, they must be assessed and analysed. This means considering the likelihood and consequence of the risk. The Risk Owner uses the **Likelihood Tool** and **Consequence Tool** to analyse the risk and understand whether the risk impact is Extreme, High, Moderate or Low. c. Evaluate Risk Risk impact evaluation allows the Risk Owner to assess whether the risk is within the tolerance or risk appetite set by CatholicCare in the Risk Appetite Statement. Once a risk treatment is applied to the risk, the Risk Owner then evaluates whether the risk is acceptable or unacceptable. If it is unacceptable, i.e. outside the risk tolerance stipulated in the Risk Appetite Statement for that category of risk, further treatment is required to make the risk acceptable. If the risk cannot be made acceptable it is not to be accepted.
4. Treat Risk	In selecting the risk treatment, Risk Owners should be proportionate in their approach. This means that they should consider cost and effort in implementing treatments and/or controls against the assessed risk level. Once controls are in place they are assessed as to whether the controls are Effective, Well Based, Improvement Desired, or Ineffective.
5. Monitor and Review	Finally, **risk is monitored using the Key Risk Indicator Summary** (Risk Category by KRI). The Senior Leadership Team monitors Key Risk Indicators, control performance and treatment plan actions for each category of risk according to a quarterly review schedule. The use of common tools and templates ensures consistent monitoring and reviews, and the **Key Risk Indicator Summary** (**Risk Category by KRI**) is used as the common reporting template throughout the Diocese.
6. Record and Report	CatholicCare maintains a Risk Register which identifies key risks. CatholicCare reports on risk according to an agreed schedule as set out under *Key Risk Register Reporting to Advisory Council* and relevant committees below.

Shared Risk - Evaluation and Assessment

Shared risk in the Diocesan context includes risks that extend across the Diocesan CSBB and CatholicCare Agencies, Chancery, schools, CatholicCare facilities or parishes. Some characteristics of a shared risk include:

- There is no natural risk owner; no one entity can manage the risk on their own.
- A network of relationships and responsibilities is present (e.g., formal, and informal relationships between schools and parishes and CatholicCare services).
- A single participant can affect the complex causes of the risk.

- Risks shared by formal agreement, or a collaborative approach.

Within the Diocese, CatholicCare, CSBB Chancery, or parishes may individually not have sufficient visibility of the risks to control the risk by themselves individually.

Effective **collaboration** and **communication** is to be used to manage the risks. As shared risk:

- Is identified, or
- Causes of the risk change, or
- Consequences of risk change, or
- Likelihood of risk change, and
- Treatments are identified or recommended or
- When the risk event has occurred

The team identifying the risk/event must advise all parties sharing the risk, then agree the treatments and ensure responsibilities are in place and followed up.

Disputed shared risk needs to be escalated for consideration jointly by the Diocesan Leadership to ensure timely treatment and monitoring.

Escalation

Residual Risk Rating	Strategy/Escalation
Extreme	• This indicates a potential breach of Risk Appetite tolerance for all risk categories. • Requires Senior Leadership team time and effort and immediate attention • Requires tailored controls that are subject to a strong monitoring regime. • Task or activity should not proceed until residual risk is reduced to an acceptable level
High	• This indicates the potential for a breach of Risk Appetite tolerance for all risk categories. • Requires Senior Leadership Team time and effort. • Requires tailored controls that are subject to a strong monitoring regime. • Task or activity may proceed but constant monitoring by Senior Leadership Team is warranted until residual risk is reduced to a more acceptable level.
Moderate	• Requires General or Executive Manager oversight and Manager level action. • If associated KRI's are outside the Risk Appetite Statement, a risk management action plan is required to show how a lower residual risk level will be achieved. • Regularly review existing controls for effectiveness and introduce additional controls if cost effective. • Tailored controls to manage risk are in place with a sound monitoring. • Task or activity can proceed upon appropriate delegated approvals.
Low	• We manage the issues as part of business as usual. • Appropriate standardised controls are likely to be in place that does not need regular monitoring. • Reviewed at least annually. • Standardised controls are likely to be in place that are monitored for conformance. • Task and activity can proceed upon appropriate delegated approvals. Senior managers should assess risk mitigation strategies to ensure we are not devoting too many resources to managing the risk too strongly. And if the risk relates to project timeframes or business development activities, consideration should be given to the possibility that we have not set ambitious enough targets.

Monitoring and Review

The Senior Leaders are to monitor KRIs, control performance, and treatment plan actions for each category of risk. The Risk Management Policy provides further information and a template for reporting risk.

Key Risk Register Reporting to Advisory Council

CatholicCare will maintain a Risk Register that identifies key strategic and operational risks. These key risks are those risk which would threaten the agency's model of operation, delivery of priorities, viability, and sustainability.

The Key Business Risk Register (KBRR) will be reported to the Finance Audit & Risk Committee at their quarterly meeting, for their review and feedback, and a more detailed review of the KBRR will be undertaken annually.

The complete risk register or Risk Management Action Plans (RMAP) (template in Risk Management Policy at *Appendix 1 - Risk Management Action Plans*) are to be included in Advisory Council papers annually.

The DGRE will receive the same reporting as the Advisory Council, along with the minutes of the Advisory Committee review outcomes.

The Executive Manager Quality Safeguarding Risk and Compliance will provide RMAPs to the DGRE at the 3rd Meeting of the Calendar Year.

Risk Closure

Key risks and risks assessed at greater than a moderate risk level in the KBRR may only be closed when the risk is no longer relevant to the strategic or operational objective, when the risk has been rated at a low level and monitoring is not deemed necessary for the objective to be achieved. Approval for risk closure must be done in consultation with the Executive Director and reported to the Senior Leadership Team. The closures should be reported in quarterly reporting.

Risk Culture

A **positive risk culture** is the desired result of implementing this Risk Management Framework. In summary it can be described as where Workers engage with risk as seamlessly as possible, and risk management is a natural attribute in our decision-making and behaviour.

CatholicCare will reflect a positive risk culture when:

- The governance structure is committed to risk management and is working as planned.
- The Senior Leadership Team is committed to risk management and promotes positive risk behaviour.
- All Workers understand risk in their roles and show a positive attitude and ownership of risk.
- Workers speak up when they are uncertain.
- Operational risk outcomes (frequency, severity) meet expectations, with few surprises.

The Senior Leadership Team direct reports are accountable as role models for the enculturation of risk management with their colleagues and stakeholders.

Related documents

- *Risk Appetite Statement*
- *Risk Management Policy*
- *Risk Management Practice Guidelines*
- *CatholicCare Advisory Council Governance Framework & Policies*

Glossary

Control

A control is a measure taken that maintains or modifies the risk.

CSBB

Catholic Schools Broken Bay

DGRE

Diocesan Governance & Risk Executive

Inherent Risk

The risk before applying any controls or risk treatments.

Key Business Risk Registers (KBRR)

Register that contains material risks which could impact the delivery of the strategic objectives.

KRI

Key Risk Indicator (s)

Operational Risk Register

A register which documents risks relevant to each operational area which may impact the strategic objectives for that operational area.

Residual Risk

The risk after considering the effects of *well-balanced*, and *effective* controls.

Risk Owner

The individual who is responsible and accountable for ensuring the risk is managed appropriately.

The level of responsibility and accountability for risk management is detailed in individual position descriptions.

Where the risk owner is the Senior Leader, this is specified in this document.

Risk Tolerance

The measure is the upper limit of the category risk appetite; once reached indicates risk is outside acceptable risk appetite.

RMAP

Risk Management Action Plan

Strategic Risk

Relates directly to CatholicCare's strategic planning and management processes. Strategic risks are those that could significantly impact on the achievement of CatholicCare's vision and strategic objectives. They are high level risks that require identification, treatment, monitoring and management by the leadership team and are set out in the Key Business Risk Register.

Sign off and review

Version	Authorised by	Approved date	Review cycle	Review due
1.0	Executive Director	7 February 2024	3 years	February 2027

Revision history

Version	Description	Author	Amendment date
1.0	Framework	Executive Manager Quality Safeguarding Risk & Compliance	7 February 2024