Risk Management Framework (Procedure)

Section 1 - Purpose

(1) The Catholic Diocese of Maitland-Newcastle (the Diocese) will manage risks to ensure we meet our mission and vision allowing us to continue to provide services to the community. We also minimise any negative impacts on the community, our people, and our operations though our risk management program.

(2) The Risk Management Framework (Framework) allows the Diocese to make decisions considering information gathered from both internal and external sources. The Framework supports organisational understanding and knowledge using risk registers, risk analysis, investigation, and data sources to identify trends, opportunities, threats, and tools developed drawing on the specific guidelines of the Australian Standard for Risk Management (AS ISO 31000:2018).

(3) Risk management plans developed by each agency reduce duplicated effort, simplify processes, and ensures a consistent approach is maintained across all business areas.

(4) Risk controls are applied and verified using electronic data management and implemented workflows to reduce potential for human error.

(5) This Framework outlines a methodical approach to managing threats to our operations and to ensure that opportunities are taken considering all applicable information to ensure we achieve our planned outcomes.

Section 2 - Scope

(6) This Framework:

a. applies to all the Diocese agencies and parishes. Risk management principles will be applied during decision making across our operations. Decisions will be made considering strategic, enterprise and operational risks that have potential to impact the community or the Diocese.
b. is designed to support the Diocese in adopting the principles of risk management as an integral part of sound management practice and an essential element of good corporate governance.
c. provides an overarching system that includes all components for managing risk within the organisation.

Section 3 - Risk Management Framework

(7) The framework includes a range of policies, guides, tools, and forms.

(8) The Head of Governance is responsible for establishing procedures to implement and maintain a risk management system. Overall responsibility for managing risk is with Directors of Agencies, clergy and through the Diocesan Leadership Group (DLG).

(9) See the link for the Risk Management Framework diagram

Section 4 - Risk Management Policy

(10) The Risk Management Policy has been established and endorsed by the Bishop and Chief Executive Officer.

(11) The Risk Management Policy serves to:

a. outline our commitment to risk management for the Diocese;
b. establish high level responsibility and accountability; and
c. include a commitment to provide resources to effectively manage risk.

(12) The Risk Management Policy will be made available to all employees via the intranet and where practicable in reception areas of our offices.

Section 5 - Risk Appetite Statement

(13) The risk appetite statement establishes a tolerable and preferred risk range. The preferred range is where the Diocese can operate without management intervention. A tolerable range is outside the preferred range; however, the activity can continue with an elevated level of management oversight. Out of tolerable range requires immediate action to bring the risk into a tolerable range or escalation to obtain agreement to accept the risk.

(14) A Risk Appetite Statement will be established and endorsed by the Chief Executive Officer and the Diocesan Leadership Group with support from the Manager, Risk & Insurance.

(15) An Agency Director may also establish risk appetite statements to meet operating contexts for each agency. The Manager, Risk & Insurance is responsible for facilitating and supporting the development of risk appetite statements.

Section 6 - Risk Assessment Template

(16) Risk Assessment Templates provide a methodical way of identification and analysis of risks and the impact those risks have on our organisation. Risk Assessor to identify control measures, actions, and monitoring requirements.

(17) Risk assessment will be conducted:

a. for all agencies;
b. for projects at the Project in a Page and Business Gate stages;
c. for incident and business continuity management;
d. as new building assets are acquired;
e. when undertaking any action which is outside “Business as Usual (BAU)” activities;
f. when proposing new services to the community; and
g. for technical functions (I.T, Finance, HR etc.) within the organisation.

(18) Agency Directors are responsible for conducting an agency risk assessment and the development of risk registers for their agencies. Managers are responsible for completing risk assessments within their area of operation. The Manager, Risk & Insurance is responsible for allocating sufficient resources to provide technical support to ensure risk assessment processes are implemented.

(19) Risk assessments will be conducted in accordance with the Risk Assessment Guide and recorded on the Risk Assessment Template.

Section 7 - Risk Register

(20) Each agency is responsible for establishing an Agency Risk Register on the approved Diocese risk assessment template. Agency Directors with support of the Manager, Risk & Insurance will identify risk in accordance with the requirements of the risk assessment guide.

(21) Risk Registers will be reviewed on an annual basis, or when:

a. material changes to operating context occurs;
b. legal obligations change;
c. incidents occur;
d. horizon scanning indicates a changed risk environment; and
e. reports from other Dioceses indicate changes to their risk profiles.

(22) The Manager, Risk & Insurance is responsible for the development of a Diocese risk assessment. The Diocese risk assessment will include enterprise risk that has potential to impact the Diocese achieving its strategic objects.

Section 8 - Agency Risk Procedures

(23) Agencies may need to adapt risk management process where legislative; compliance or technical requirements apply.

(24) The Manager, Risk & Insurance is responsible for providing technical support and working with agency subject matter experts to integrate the risk management program into agency processes.

(25) Examples of these areas are:

a. Work Health and Safety;
b. Project Management;
c. Information Technology / Cyber Security; and
d. Financial Services.

(26) Agency processes will provide additional level of detail specific to the agency’s needs and will be translatable into the Diocese risk program.

Section 9 - Agency Risk Management Plans

(27) Risk management plans identify initiatives that assist the Diocese and agencies to manage risk. Initiatives range between short- and long-term projects. Each initiative has defined outcomes, is allocated a budget, a sponsor and monitored as part of reporting processes.

(28) Each Agency Director will develop a risk management plan with support from the Safety and Risk Partner, and the risk management plan template.

(29) Agency Directors are responsible for facilitating the development of risk management plans. Actions within risk management plans will have responsibility assigned to senior managers within the agency.

(30) The Risk Management Plan will:

a. provide a summary of key risks, review of incidents, and control breakdowns;
b. identify priority risks and treatment actions;
c. provide an overview of risk maturity in the agency and activities;
d. define key risk monitoring activities; and
e. define key risk indicators and cycles to assess performance and culture.

(31) Risk Management Plans will be reviewed and updated on an annual basis in line with organisational planning cycles by the Agency Directors and the Safety and Risk Partner. Where heightened residual risks or emerging risks are identified, these will be escalated to the Manager, Risk & Insurance.

Section 10 - Reporting and Notification

(32) Data and reporting are a component our governance obligations and allows us to make informed decisions on the direction of the Diocese and our agencies.

(33) The following table defines data and reporting.

Type	Information reported	Audience	Content
Real time data	Agency risk information via dashboard Actions registers Risk trends	Agency Directors Operational Management Group (OMG)	Overview of agency operational and enterprise risk. Actions status
Quarterly reporting	Diocese risk Agency top risks Thematic analysis Risk trend Actions status Progress of initiatives from risk management plans	Diocese Audit and Risk Committee CEO	Data on risk profiles Strategic and enterprise risk rated high and above Trends and themes Actions due / overdue / complete statistics
Annual Review	Agency risk analysis	Agency Directors	Agency risk information to support the development and review of risk management plans.

(34) he Safety and Risk Partner is responsible for the development of agency and Diocese risk dashboards.

(35) Agency Directors are responsible for providing risk reports on a quarterly basis to the Manager, Risk & Insurance for submission to the Diocesan Audit and Risk Committee (DARC). The Manager, Risk & Insurance is responsible for the development of a risk summary as part of the DARC report with final responsibility resting with the Head of Governance for presentation to the appropriate parties.

Section 11 - Escalation

(36) When risk is first identified, or when changing circumstances increase the residual risk rating this information is reported in accordance with the Risk Assessment Guide.

Section 12 - Capability and Culture

(37) Capability and training programs, Governance will maintain communication systems, guides, tools, and forms to ensure a best practice risk culture is developed and maintained throughout the Diocese.

(38) Annually, the Manager, Risk & Insurance will conduct a review of the Framework using defined criteria (such as

ACNC, Commonwealth or NSW Government assessment tools).

(39) Actions to improve capability and culture within the Diocese will be developed from the findings of the assessment.

(40) The Head of People and Culture maintains a training needs analysis, training materials, training calendar and online learning system with support from the Manager, Risk & Insurance.

Section 13 - Framework Evaluation, Review and Improvement

(41) Annually, the Manager, Risk & Insurance will maintain a report that summarises the performance of the Framework.

(42) The report will include:

a. conformance of program against compliance body obligations;
b. changes required by legislation;
c. summary of risk management plans and performance of initiatives;
d. results of the annual capability and culture review;
e. risk trends;
f. risk horizon; and
g. verification programs (internal audit).

(43) The Manager, Risk & Insurance will develop and document strategies for improving the Framework throughout the Diocese.

Section 14 - Diocese Audit and Risk Committee

(44) The Bishop establishes an Audit and Risk Committee to provide independent assurance and advice to the Bishop on the Diocese's risk, control and compliance framework and its financial statement responsibilities.

(45) The Chief Executive Officer will ensure necessary resources are provided to support the Diocesan Audit and Risk Committee (DARC).

(46) DARC Terms of Reference will include:

a. authority of the committee;
b. composition and tenure;
c. responsibilities;
d. reporting;
e. confidentiality and security;
f. meeting frequency; and
g. administrative arrangements.

(47) DARC review and oversight functions include:

a. risk management;

b. internal controls;
c. financial statements;
d. legislation and policy requirements;
e. internal audit;
f. external audit;
g. governance arrangements; and
h. other responsibilities required by the bishop.

Section 15 - Responsibilities

Position	Responsibilities
Bishop	Establishing and endorsing a Risk Management Policy. Establish an Audit and Risk Committee.
Chief Executive Officer (CEO)	Establishing and endorsing a Risk Management Policy. Establishment of a risk appetite statement. Establishing actions to manage escalated risk. Ensure necessary resources are provided to support the Diocesan Audit and Risk Committee (DARC).
Diocesan Leadership Group (DLG)	Endorsing risk appetite statement.
Agency Directors	Establish a risk appetite statement as needed for their agency. Conducting an agency risk assessment and development of risk registers for their agencies. Develop a Risk Management Plan for their agency. Review and monitor the implementation and effectiveness of risk management plans. Provide risk reports on a quarterly basis to the Risk and Compliance Manager for submission to the DARC. Establishing actions to manage escalated risk.
Managers	Identification of risk associated with their area of responsibility and report this to Agency Directors, as necessary. Establishing actions to manage escalated risk.
Head of People and Culture	Develop and maintain a training needs analysis, training materials, training calendar and online learning systems.
Head of Governance	Supporting the establishment of a risk appetite statement.
Manager, Risk & Resolutions	Establishing procedures to implement and maintain a risk management program. Providing technical support to establish risk appetite statement/s. Allocating sufficient resources to provide technical support to ensure risk assessment processes are implemented. Providing technical support and working with agency subject matter experts to integrate the risk management program into agency processes. Assist agencies to review and monitor the implementation and effectiveness of risk management plans. Develop and provide a risk summary as part of the DARC report. Review annually the risk management program using defined criteria and provide a report to improve the risk management program. Support the Head of People and Culture to maintain a training needs analysis, training materials, training calendar and online learning system.

Section 16 - References

(48) ASO ISO 31000:00 (Approved on behalf of the Council of Standards Australia – 19 September 2018).

Section 17 - Review

(49) The Diocese Policy Management Policy and Diocese Policy Management Procedures govern the development, approval, implementation and ongoing management of policies, procedures and supporting documents.

(50) The document will be reviewed when there is a legislative change, organisational change, delegations change or at least every 3 years to ensure it continues to be current and effective.

Status and Details

Status	Current
Effective Date	3rd April 2024
Review Date	11th March 2025
Approval Authority	Manager Risk & Insurance
Approval Date	11th October 2022
Expiry Date	To Be Advised
Unit Head	Megan Grainger Head of Governance
Enquiries Contact	Risk & Insurance

Glossary Terms and Definitions

"Bishop" - Bishop means the diocesan bishop of the Catholic Diocese of Maitland-Newcastle who has taken canonical possession of the Diocese in accordance with the Code of Canon Law in force ("the Code"). Bishop has the meaning pursuant to section 2 of the Roman Catholic Church Trust Property Act (NSW) 1936 ("the Act"). Under the Act, the Bishop of the Diocese and the Diocesan College of Consultors collectively are the body corporate of the Trustees. If the episcopal see comprising the Diocese is either impeded or vacant as set out in the Code, then the Bishop of Maitland-Newcastle shall be inclusive of the person properly empowered to undertake the governance of the impeded or vacant see of Maitland-Newcastle in accordance with the Code, including: ♦ a coadjutor bishop; ♦ an auxiliary bishop; ♦ the diocesan administrator; and ♦ an apostolic administrator.

"Agency" - Diocesan agencies may also be referred to as directorates. Diocesan agencies are intra-diocesan organisational structures that have been established and developed in the life of the church, to undertake good works and services on behalf of the Diocese and have the capacity to bind the Diocese to its actions. For the most part, but not exclusively, diocesan agencies are led by executive directors. Examples of Diocesan agencies include: ♦ CatholicCare Social Services Hunter-Manning including the Development and Relief Agency (DARA); ♦ Catholic Development Fund; ♦ Catholic Schools Office and the diocesan systemic schools; ♦ Hunter Community Housing; ♦ Office of Safeguarding; ♦ Pastoral Ministries; ♦ St Nicholas services including Early Education centres and Out of School Hours Care (OOSH) services; and ♦ Shared Services, which is inclusive of multiple specialist tertiary providers to diocesan parishes and agencies, that forms part of the Diocesan Curia.

"Catholic Diocese of Maitland-Newcastle (the Diocese)" - The Catholic Diocese of Maitland-Newcastle (the Diocese) is inclusive of all parishes and agencies, communities, ministries and works that are under the authority of the Bishop of Maitland-Newcastle. The Bishop takes his authority from Canon Law (Canons 375-402). The geographical coverage of the Diocese includes all or part of the Newcastle, Lake Macquarie, Maitland, Cessnock, Port Stephens, Singleton, Muswellbrook, Upper Hunter, Dungog and Mid-Coast local government areas, with almost 160,000 Catholics, 38 parishes and serviced by multiple diocesan ministries and agencies. The Diocese is not wholly geographic in nature. There are elements of the Catholic Church operating within the physical boundaries of the Diocese that do not fall under the authority of the Bishop and are not a part of the Diocese. Equally, particular diocesan ministries occur within external institutions (e.g. Prison Chaplaincy, Hospital Chaplaincy).

"Diocesan Leadership Group (DLG)" - The Diocesan Leadership Group meets regularly to provide a consultative forum so that mission, pastoral and strategic plans and decisions for the diocese are realised to the highest standard.

"Directors of Agency" - Means the director or most senior staff member of any agency of the Diocese.

"Risk Management" - Risk management is the identification, assessment, and prioritisation of risks followed by

coordinated and economical application of resources to minimise, monitor, and control the probability and /or impact of unfortunate events or to maximise the realisation of opportunities. Risk management incorporates the Diocese's readiness and capacity to accept risks as an inescapable part of undertaking its mission. Risk management's objective is to assure uncertainty does not deflect the endeavour from its missionary or business goals.

"Control" - The measure that maintains and/ or modifies risk.

"Monitoring" - The continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

"Residual risk" - The risk remaining after risk treatment.

"Review" - Activity undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve the established objectives.

"Risk analysis" - The process to comprehend the nature of risk and to determine the level of risk.

"Risk appetite" - The amount of risk that the Diocese is prepared to accept or be exposed to at any point in time.

"Risk assessment" - The overall process of risk identification, risk analysis and evaluation.

"Risk management plan" - Scheme within the risk framework specifying the approach, the managment components, and resources to be applied to the managment of risk.

"Risk profile" - The description of any set of risks.

"Risk management process" - The systematic application of management policies, framework, and practices to the activities of communicating, consulting, establishing the context, identifying analysing evaluating, treating, monitoring, and reviewing risk.