DIOCESAN COUNCIL
POLICY 39

Anglican Church Diocese of Perth

Risk Management

Approved by: Diocesan Council 17 December 2015

1 PREAMBLE

The Perth Diocesan Trustees under the authority of the Diocesan Trustees Statute 1952 have the responsibility for providing risk management structures for the Diocese and has oversight in these matters.

2 THEOLOGY

As Christians, scripture calls us to be faithful stewards of that which God entrusts to our care. This includes not only people but property and all God's creation. This policy is aimed at mitigating the risk associated with life and action in the Diocese.

3 DEFINITION

Clergy or member of the clergy – means a person in Holy Orders ordained in this Church or in another Church in communion with this Church and clerical has the same meaning

Church – means the Anglican Church of Australia within this Diocese

Church authority – means the Archbishop or a person or entity having administrative authority of or in a Church entity to licence, appoint, authorise, dismiss or suspend a Church worker or Church volunteer

Church entity – means an unincorporated entity including a committee, commission, a parish or parish council in the Diocese, the Cathedral or Chapter of the Cathedral, that exercises ministry within, or on behalf of, the Church with actual or apparent authority of the Church

Church volunteer – means a person aged 18 or more years who is not a Church worker but who:

(a) holds a voluntary role, office or position in a congregation or parish or in the Cathedral; or
(b) holds otherwise any specific voluntary role, office or position in the Diocese with actual or apparent authority of the Church

Church worker: - means any person who is or at any relevant time was:

(a) a member of the Clergy (including the Dean of the Cathedral) whether or not holding the Archbishop's licence or permission to officiate;
(b) employed or engaged by a Church authority or Church entity; or
(c) holding a position or performing a function whether voluntary or for payment with the actual or apparent authority of a Church authority of Church entity

Diocese: - means the Diocese of Perth

Diocesan Council – means the Council of the Diocese established pursuant to the Diocesan Council Statute 1888

Diocesan secretary: - means the person appointed by the Trustees as Secretary or as acting Secretary for the time being

Risk: - means the effect or uncertainty on objectives.

(a) an effect is a deviation from the expected – positive or negative.
(b) objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product or process).

Risk Appetite – means level of risk as quantified by the Perth Diocesan Trustees

Risk Management: - means coordinated activities to direct and control a Church authority or Church entity with regard to risk.

Risk Management Framework: - means the document shown at Appendix 1 pf this policy

Risk Management Process: - means systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Trustees: - shall mean The Perth Diocesan Trustees pursuant to The Diocesan Trustees Statute 1888

4 SCOPE

This policy applies to clergy, Church workers and Church volunteers within the Diocese, and to all Diocesan and parish property.

5 POLICY

The Diocese aims to achieve best practice, aligned with AS/NZS ISO 31000:2009 Risk Management, in the management of all risks that may affect the Diocese and its clergy, Church workers and Church volunteer's assets, functions, objectives, operations or members of the public.

The provisions of this policy can be found in the Risk Management Framework at Appendix 1 of this policy.

The Diocesan Secretary will have the overall responsibility for implementation, monitoring objectives and procedures, as well as, communication of this policy, objectives and procedures, throughout the Diocese. Where appropriate the Diocesan Secretary will delegate the implementation and monitoring to the management team.

Clergy, and Church volunteers within the Diocese are recognised as having a role in risk management process from the identification of risks to implementing risk treatments and shall be invited and encouraged to participate in the process.

Consultants may be retained at times to advise and assist in the risk management process, or management of specific risks or categories of risk. Appropriate training will be provided, refer to the Risk Manager.

6 RESPONSIBILITIES

The Diocesan Secretary is responsible for the implementation of the risk management objectives and procedures.

All Church workers and Church volunteers are responsible for managing risks in their areas.

7 PROCESS

A risk management framework has been established, based on the Australian Standard AS/NZS ISO 31000:2009.

8 RISK MANAGEMENT OBJECTIVES

Risk management objectives are to:

(a) protect people and property from harm and damage;
(b) provide transparent and formal oversight of the risk and control environment to enable effective decision making;
(c) embed appropriate and effective controls to mitigate risk into all activities rather than being seen as a separate function;
(d) make timely involvement of the appropriate stakeholders and decision makers at all levels to ensure risk management remains relevant and up-to-date;

(e) achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations;
(f) to enhance risk versus return within our risk appetite;
(g) enhance organisational resilience;
(h) aligned with the external and internal context and risk profile; and
(i) identify and provide for the continuity of critical operations.

9 RISK APPETITE

The Trustees have quantified the Diocesan risk appetite through the development and approval of Risk Assessment and Acceptance Criteria. The criteria are included within the Diocesan Risk Management framework and are subject to ongoing review in conjunction with this policy.

All Diocesan risks to be reported at The Trustees and Diocesan Council. Levels of risk are to be assessed according to the Diocesan Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as special projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be approved by the Diocesan Secretary and utilised.

10 MONITORING AND REVIEW

The Diocesan Secretary will implement and integrate a monitor and review process to report to The Trustees, covering the achievement of the Risk Management objectives, the management of individual risks and the ongoing identification of issues and trends. The Trustees will report and make recommendations to Diocesan Council for mitigation of risk.

This policy will be reviewed at least every three years by the Trustees Audit and Risk Committee. Any changes necessary to this Policy will be reported to the Trustees and Diocesan Council for approval.

11 FURTHER INFORMATION

For further information on this policy and the risk management procedures, contact the Diocesan Secretary at the Diocesan Office.

Risk Management Framework

Anglican Church, Diocese of Perth

November 2015

Final

Table of Contents

Introduction

This Risk Management Framework (framework) sets out the Anglican Diocese of Perth approach to the identification, assessment, management, reporting and monitoring of risks. The framework and risk management procedures (procedures) contained within this document are aligned with AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines.

It is essential that all areas of the Anglican Diocese of Perth adopt this framework to ensure:

- Strong corporate governance
- Compliance with relevant legislation, regulations and internal policies
- Planning and reporting requirements are met
- Uncertainty and its effects on objectives is understood

The framework and procedures aim to balance a documented, structured and systematic process with the size and complexity of the Anglican Diocese of Perth along with existing time, resource and workload pressures.

For further information on the framework, policy or procedures contact the Diocesan Secretary.

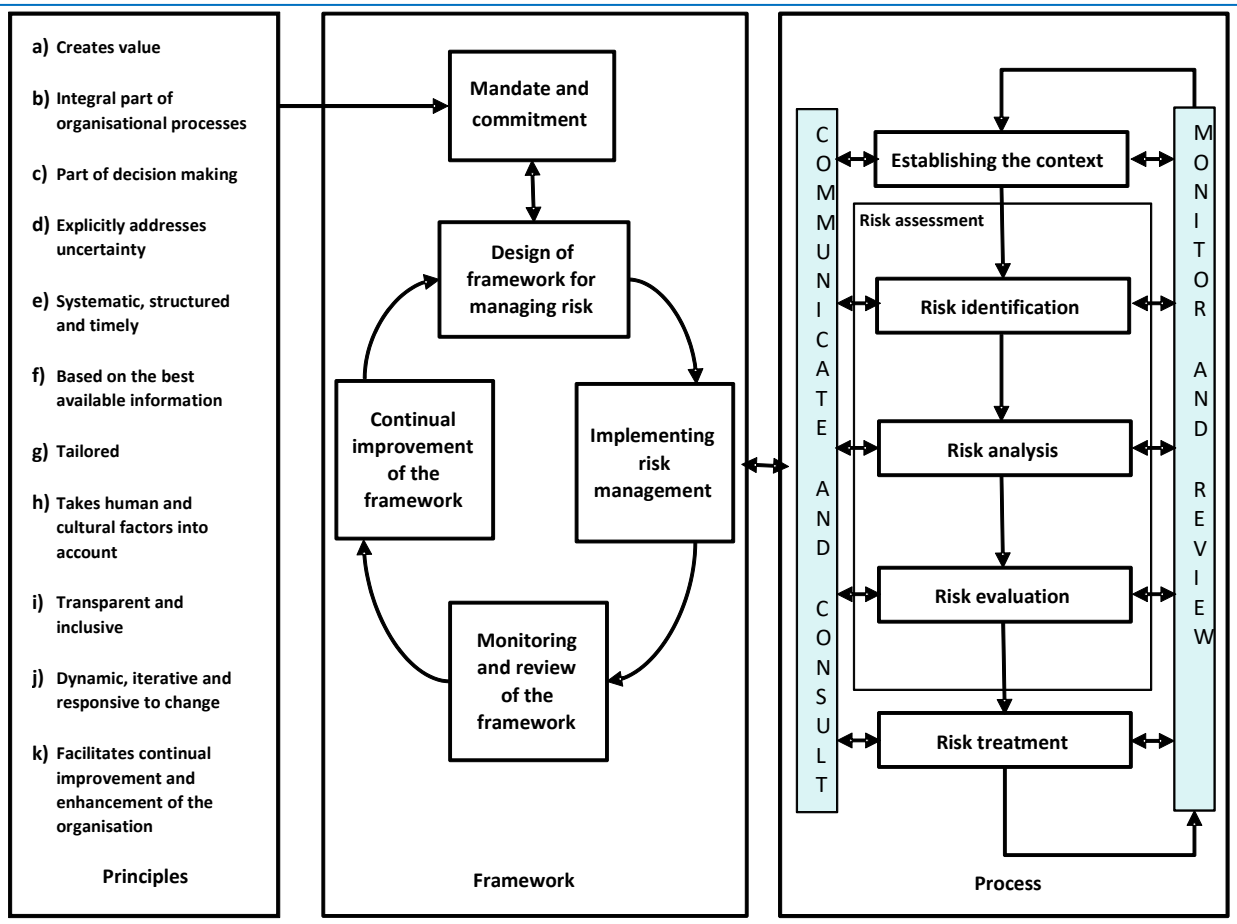

Diagram 1: Risk Management Process (Source: AS/NZS 31000:2009)

Risk Management Policy

Purpose

The Anglican Diocese of Perth Risk Management Policy documents the commitment and objectives regarding managing uncertainty that may impact the Anglican Diocese of Perth vision, mission, strategies, goals or objectives.

Policy

The Anglican Diocese of Perth aims to achieve best practice, aligned with AS/NZS ISO 31000:2009 Risk Management, in the management of all risks that may affect the Anglican Diocese of Perth, clergy, lay employees, parishioners, volunteers, assets, functions, objectives, operations or members of the public.

The Audit and Risk Management Committee of The Perth Diocesan Trustees will review this Policy and recommend approval to The Perth Diocesan Trustees and Diocesan Council.

The Diocesan Secretary will have the overall responsibility for implementation, monitoring Objectives and Procedures, as well as communication of this policy throughout the Anglican Diocese of Perth. Where appropriate the Diocesan Secretary will delegate the implementation and monitoring to his management team.

Clergy, lay employees and volunteers within the Anglican Diocese of Perth are recognised as having a role in risk management process from the identification of risks to implementing risk treatments and shall be invited and encouraged to participate in the process.

Consultants may be retained at times to advise and assist in the risk management process, or management of specific risks or categories of risk.

Definitions (from AS/NZS ISO 31000:2009)

Risk: Effect of uncertainty on objectives.

Note 1: An effect is a deviation from the expected – positive or negative.

Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product or process).

Risk Management: Coordinated activities to direct and control an organisation regarding risk.

Risk Management Process: Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Objectives

- Protect people and property from harm and damage.
- Provide transparent and formal oversight of the risk and control environment to enable effective decision making.
- Embed appropriate and effective controls to mitigate risk into all activities, rather than being a separate function.
- Appropriate and timely involvement of stakeholders and decision makers at all levels to ensure risk management remains relevant and up-to-date.
- Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.
- Enhance risk versus return within our risk appetite.
- Enhance organisational resilience.
- Aligned with the external and internal context and risk profile.
- Identify and provide for the continuity of critical operations.

Risk Appetite

The Perth Diocesan Trustees has quantified the Anglican Diocese of Perth risk appetite through the development and approval of Risk Assessment and Acceptance Criteria. The criteria are included within the Anglican Diocese of Perth Risk Management Framework and are subject to ongoing review in conjunction with the Risk Management Policy.

All Diocesan risks to be reported at The Perth Diocesan Trustees and Diocesan Council level are to be assessed according to the Anglican Diocese of Perth Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as special projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be approved and utilised.

Monitor & Review

The Diocesan Secretary will implement a monitoring and review process to report to The Perth Diocesan Trustees, covering the achievement of the Risk Management Objectives, the management of individual risks and the ongoing identification of issues and trends. The Perth Diocesan Trustees will report and make recommendations to Diocesan Council for mitigation of risk.

This policy will be reviewed at least every three years by the Perth Diocesan Trustees via the Audit and Risk Committee.

Further Information

For further information on this policy, contact the Diocesan Secretary.

Governance

Appropriate governance of risk management within the Anglican Diocese of Perth provides:

- Transparency of decision making
- Clear identification of the roles and responsibilities of the risk management functions
- An effective governance structure to support the risk framework

Framework Review

The Risk Management Framework is to be reviewed for appropriateness and effectiveness at least once every three years.

Operating Model

The Anglican Diocese of Perth has adopted a "Three Lines of Defence" model for the management of risk. This model ensures roles; responsibilities and accountabilities for decision making are structured to demonstrate effective governance and assurance. By operating within the approved risk appetite and framework, The Perth Diocesan Trustees will have assurance that risks are managed effectively to support the delivery of the:

- Anglican Diocese of Perth Mission Plan
- Ongoing Operations of Worshipping Communities, Trusts and other organisations
- Special Projects

First Line of Defence

All operational areas of the Anglican Diocese of Perth are considered '1st Line'. They are responsible for ensuring that risks (within their scope of operations) are identified, assessed, managed, monitored and reported. Ultimately, they bear ownership and responsibility for losses or opportunities from the realisation of risk. Associated responsibilities include;

- Establishing and implementing appropriate processes and controls for the management of risk (in line with this framework).
- Undertaking adequate analysis to support the decisions on risk matters.
- Reviewing controls.
- Put in place risk mitigation strategies where necessary, based on level of residual risk. If needed escalate to the Diocesan Secretary if risk treatment solutions cannot be implemented.
- Retain primary accountability for the ongoing management of their risk and control environment.

Second Line of Defence

The Diocesan Secretary and the Diocesan Registrar / Archdeacons, supported by the Diocesan Council and the Management Team is the primary '2nd Line'. The Diocesan Secretary owns and manages the framework for risk management and the Archdeacons work with the Worshipping Communities. They draft and implement the policy and statutes and provide the necessary tools and training to support the 1st line process.

By maintaining oversight on the application of the framework they provide a transparent view and level of assurance to the 1st and 3rd lines of the risk and control environment. Additional responsibilities include:

- Providing independent oversight of risk matters as required.
- Monitoring and reporting on emerging risks.
- Co-ordinate Anglican Diocese of Perth risk reporting.

Third Line of Defence

External Audit & Internal Audits (where appropriate) are the third line of defence, providing independent assurance to the Audit and Risk Committee of The Perth Diocesan Trustees and Senior Management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

Internal Audit – Appointed by the Diocesan Secretary from time to time to report on the adequacy and effectiveness of internal control processes and procedures. The scope of which would be determined by the Diocesan Secretary with input from the Audit and Risk Committee.

External Audit – Appointed by the Synod on the recommendation of the Audit and Risk Committee of The Perth Diocesan Trustees to report independently to The Perth Diocesan Trustees on the annual financial statements.

Governance Structure

The following diagram depicts the governance and reporting structure for risk management within the Anglican Diocese of Perth.

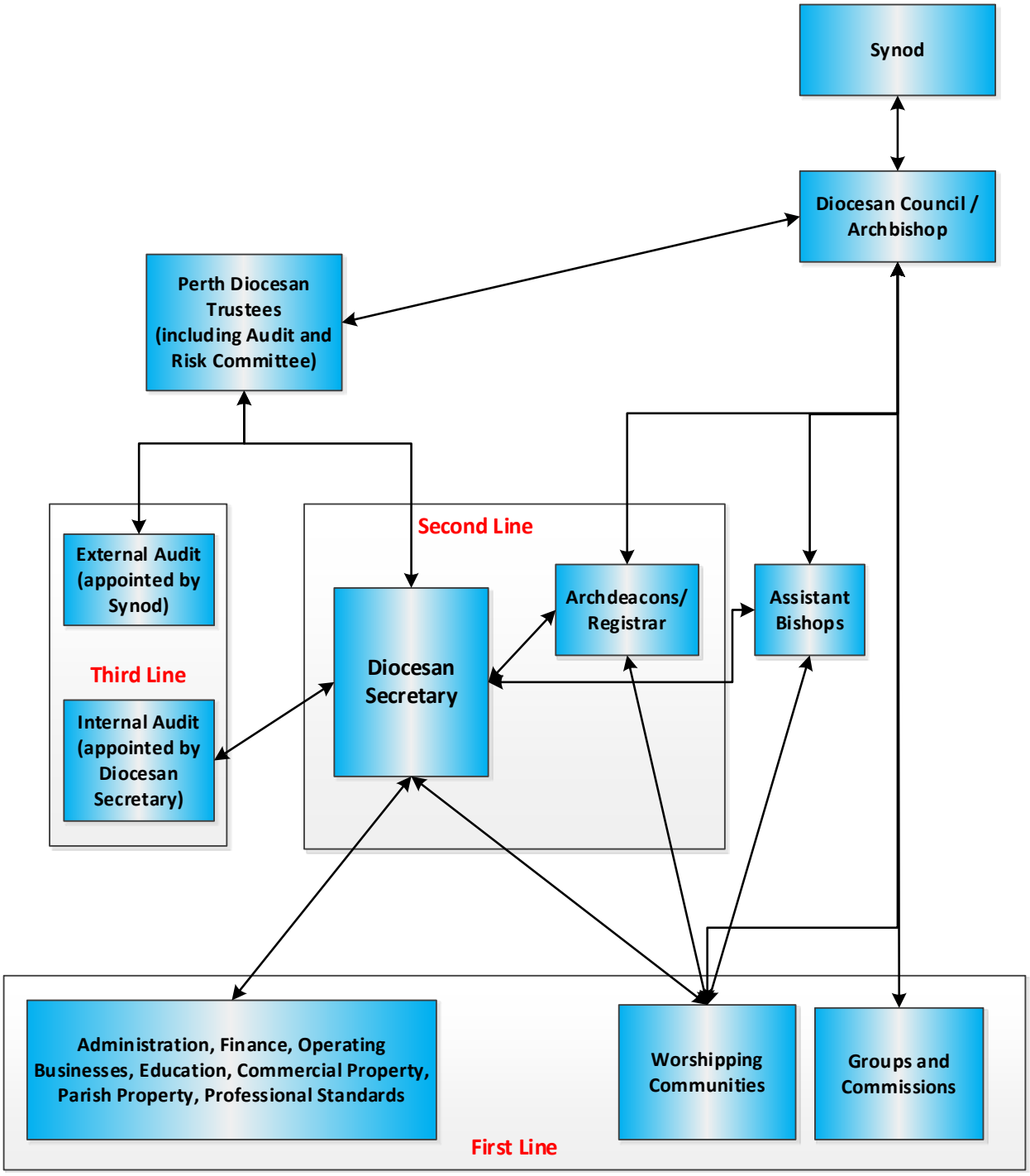

Diagram 2: Risk Management Governance Structure

Roles & Responsibilities

The Perth Diocesan Trustees

- The responsible corporate entity within the Anglican Diocese of Perth for all risk and liability matters
- Review and approve the Anglican Diocese of Perth Risk Appetite and Risk Management Framework and ensure where possible appropriate mitigation strategies are implemented
- Establish and maintain an Audit and Risk Committee

Audit and Risk Committee of The Perth Diocesan Trustees

- Support the Trustees and Diocesan Council to provide effective corporate governance
- Oversight of all matters that relate to the conduct of External Audits
- Is independent, objective and autonomous in deliberations
- Make recommendations to The Perth Diocesan Trustees on External Auditor appointments for approval by Synod

Diocesan Council

- Own and manage the Risk Profiles at Business Unit under its control particularly for Worshipping Communities and Groups and Commissions
- Drive risk management culture within the Diocese, particularly within Worshipping Communities and Groups and Commissions reporting to Diocesan Council
- Diocesan Council to drive risk management culture with appropriate policies and statues with Episcopal support through the Assistant Bishops and Archdeacons / Registrar.
- Highlight any emerging risks or issues accordingly
- Incorporate ‘Risk Management’ into Diocesan Council Meetings

Diocesan Secretary

- Appoint Internal Auditors as required
- Liaise with The Perth Diocesan Trustees in relation to risk acceptance requirements
- Review the effectiveness of the Risk Management Framework
- Drive consistent embedding of a risk management culture
- Analyse and discuss emerging risks, issues and trends
- Document decisions and actions arising from ‘risk matters’
- Own and manage the Risk Profiles.

Diocesan Secretary and Leadership Team

- Own and manage the Risk Profiles at Business Unit level.
- Drive risk management culture within Business Units.
- Highlight any emerging risks or issues accordingly.
- Incorporate 'Risk Management' into Executive Leadership Team Meetings, by incorporating the following agenda items;
    - New or emerging risks
    - Review existing risks
    - Control adequacy
    - Outstanding issues and actions

Worshipping Communities, Business Units, Groups and Commissions

- Own, manage and report on specific risk issues as required.
- Assist in the Risk & Control Management process as required.
- Drive risk management culture within Worshipping Communities, Business Units, Groups and Commissions.

Document Structure

The following diagram depicts the relationship between the Risk Management Policy, procedures and supporting documentation and reports. In addition, it also shows a 'sibling' relationship with other Anglican Diocese of Perth Policies that integrates with Risk Management principles and approach.

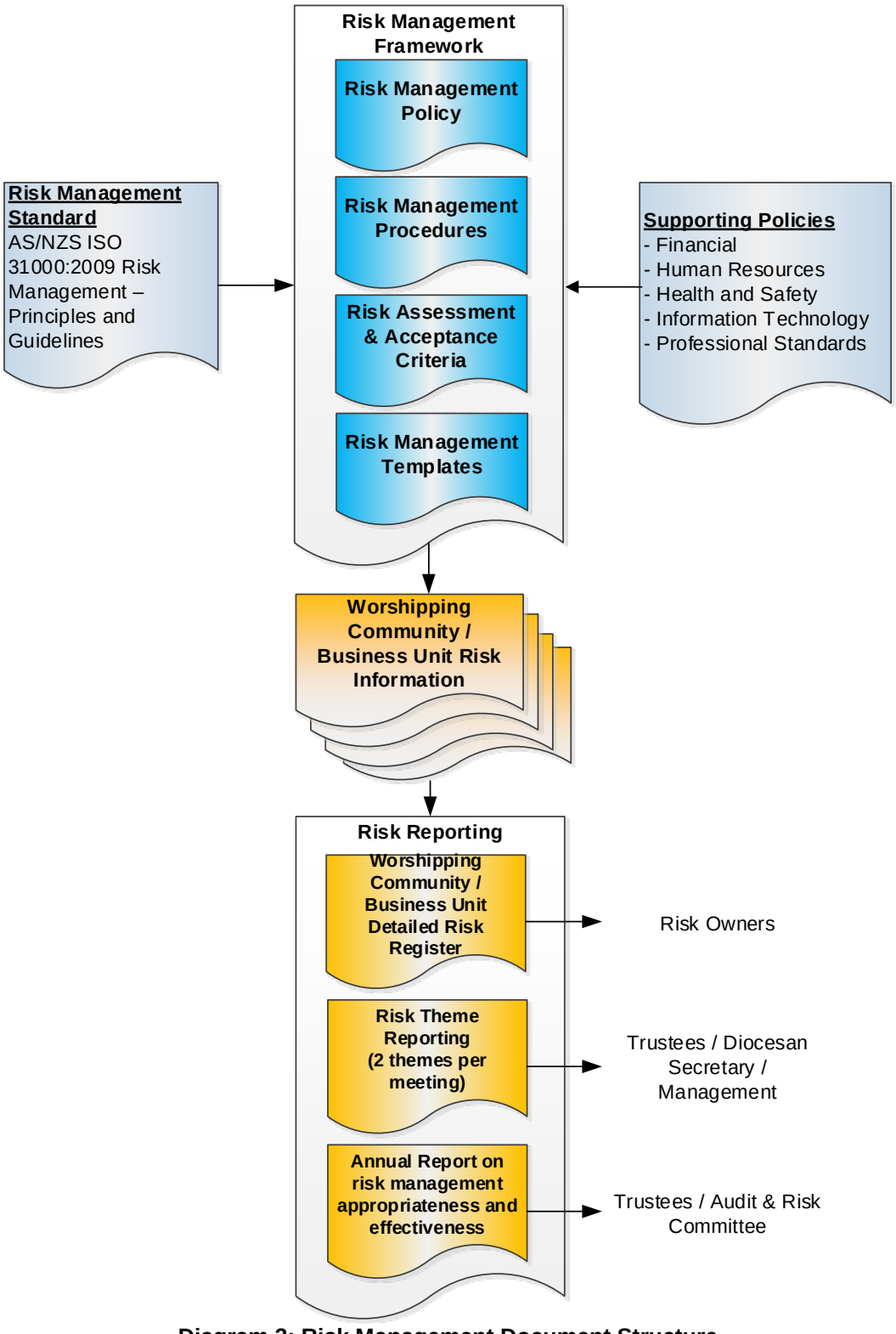

Diagram 3: Risk Management Document Structure

Risk Management Procedures

All Managers, Business Units and Worshipping Communities of the Anglican Diocese of Perth are required to assess and manage their risk profiles on an ongoing basis.

Each Manager is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Business Unit / Worshipping Community.
- Reviewed on at least an annual basis, unless there has been a material restructure or change in the risk and control environment.
- Maintained in the standard format.

This process is supported by the use, workshops and ongoing engagement.

Risk Management Process

To ensure alignment with ISO 31000:2009 Risk Management, the following approach is to be adopted for all risk assessments.

Establishing the Context

The first step in the risk management process is to understand the context within which the risks are to be assessed and what is being assessed, this forms two elements:

Organisational Context

The Anglican Diocese of Perth Risk Management Procedures provides the basic information and guidance regarding the organisational context to conduct a risk assessment; this includes Risk Assessment and Acceptance Criteria (Appendix A). In addition, existing Risk Themes are to be utilised (Appendix B) where possible to assist in the categorisation of related risks.

Any changes or additions to the Risk Themes must be approved by the Diocesan Secretary.

All risk assessments are to utilise these documents and templates to allow consistent and comparable risk information to be developed and considered within planning and decision-making processes.

Specific Risk Assessment Context

To direct the identification of risks, the specific risk assessment context is to be determined prior to and used within the risk assessment process. For risk assessment purposes the Anglican Diocese of Perth has been divided into four levels of risk assessment context:

Strategic Context

Refers to the organisations external environment and high-level direction. Inputs to establishing the strategic risk assessment context may include;

- The Diocese Vision / Mission Plan
- Stakeholder Analysis
- Environment Scan / SWOT Analysis
- Existing Strategies / Objectives / Goals

Operational Context

Refers to the day to day activities, functions, infrastructure and services of the Diocese. Prior to identifying operational risks, the operational area should identify its Key Activities in delivering its Mission. i.e. what is trying to be achieved.

Project Context

Project Risk has two main components:

- **Risk in Projects** refers to the risks that may arise because of project activity (i.e. impacting on process, resources or IT systems) which may prevent the Anglican Diocese of Perth from delivering its Mission.
- **Project Risk** refers to the risks which threaten the delivery of project outcomes.

Hazard Context

This refers to direct physical threats, hazards or vulnerabilities that may harm persons and/or cause loss and damage.

In addition to understanding what is to be assessed, it is also important to understand who are the key stakeholders or areas of expertise that may need to be included within the risk assessment.

Risk Identification

Using the specific risk assessment context as the foundation and in conjunction with relevant stakeholders, answer the following questions, capture and review the information within each Risk Profile.

- What can go wrong? / What are areas of uncertainty and how does this impact? (Risk Description)
- How may this risk eventuate? (Causal Factors)
- What are the potential consequential outcomes of the risk eventuating? (Resulting In)
- What Risk Theme best applies to the Risk Description? (Risk Theme)
- What are the current measurable activities that mitigate this risk from eventuating? (Existing Controls)

Risk Analysis

To analyse the risks the Anglican Diocese of Perth Risk Assessment and Acceptance Criteria (Appendix A) is applied:

Inherent Risk Rating

- Determine relevant consequence categories and rate how bad it could be if the risk eventuated without existing controls in place (Consequence)
- Determine how likely it is that the risk will eventuate to the determined level of consequence without existing controls in place (Likelihood)
- By combining the measures of consequence and likelihood, determine the inherent risk rating (Level of Risk)

Assessed Risk Rating

- Based on the documented existing controls, analyse the risk in terms of Existing Control Ratings (Overall Control Rating)
- Determine relevant consequence categories and rate how bad it could be if the risk eventuated with existing controls in place (Consequence)
- Determine how likely it is that the risk will eventuate to the determined level of consequence with existing controls in place (Likelihood)
- By combining the measures of consequence and likelihood, determine the assessed risk rating (Level of Risk)

Risks are not analysed until the existing controls have been taken into account. Accordingly, the first step is to identify existing controls and understand their role in influencing the likelihood and consequence measures. Controls are those things that limit likelihood and consequence, and include such things as training, management overview, succession planning, passwords, disaster recovery planning, business planning, safety management, etc. The Risk key controls are defined as being:

- Preventative – all about preventing the risk from occurring and limit likelihood
- Detective and Responsive – about identifying the risk as it occurs and rectifying or limiting the consequences

Risk Evaluation

The Risk Owner is to verify the risk analysis and make a risk acceptance decision based on:

- Controls Assurance (i.e. are the existing controls in use, effective, documented, up to date and relevant)
- Existing Control Rating
- Level of Risk
- Risk Acceptance Criteria (Appendix A)
- Risk versus Reward / Opportunity

The risk acceptance decision needs to be captured within the risk register and those risks that are acceptable are then subject to the monitor and review process.

Note: A Risk Owner at this point may need to escalate a risk to the Diocesan Secretary due to its urgency, level of risk or systemic nature.

Risk Treatment

For risks deemed unacceptable, determine risk treatment options that may improve existing controls and/or reduce consequence / likelihood to an acceptable level.

Risk treatments may involve actions such as avoid, share, transfer or reduce the risk with the treatment selection and implementation to be based on;

- Cost versus benefit
- Ease of implementation
- Alignment to the Diocese Mission

For risk treatments that fall outside risk owners delegated level of authority, a formal risk treatment plan is to be developed for endorsement.

Once a treatment has been fully implemented, the Risk Owner is to review the risk information and acceptance decision with the treatment now noted as a control and those risks that are acceptable then become subject to the monitor and review process.

Monitoring & Review

Risk Owners to review their acceptable risks at least on an annual basis or if triggered by one of the following; changes to context, new information is available, a treatment is implemented, an incident occurs or due to audit/regulator findings.

Risk Owners are to monitor the status of risk treatment implementation and report on, if required.

The Diocesan Secretary will monitor and report on significant risks and treatment implementation as part of their normal Perth Diocesan Trustees agenda item with specific attention given to risks that meet any of the following criteria:

- Risks with a Level of Risk of High or Extreme
- Risks with Inadequate Existing Control Rating
- Risks with Consequence Rating of Catastrophic
- Risks with Likelihood Rating of Almost Certain

The design and focus of Risk Summary reports will be determined from time to time on the direction of the Audit and Risk Committee of The Perth Diocesan Trustees who will also monitor the effectiveness of the Risk Management Framework ensuring it is practical and relevant to the organisation.

Communication & Consultation

Throughout the risk management process, stakeholders will be identified, and where relevant, be involved in or informed of outputs from the risk management process.

Risk management awareness and training will be provided to all staff and key volunteers.

Risk management will be included within the employee induction process to ensure new employees are introduced to the Anglican Diocese of Perth risk management culture.

Reporting Requirements

Coverage & Frequency

The following diagram provides a high-level view of the ongoing reporting process for Risk Management

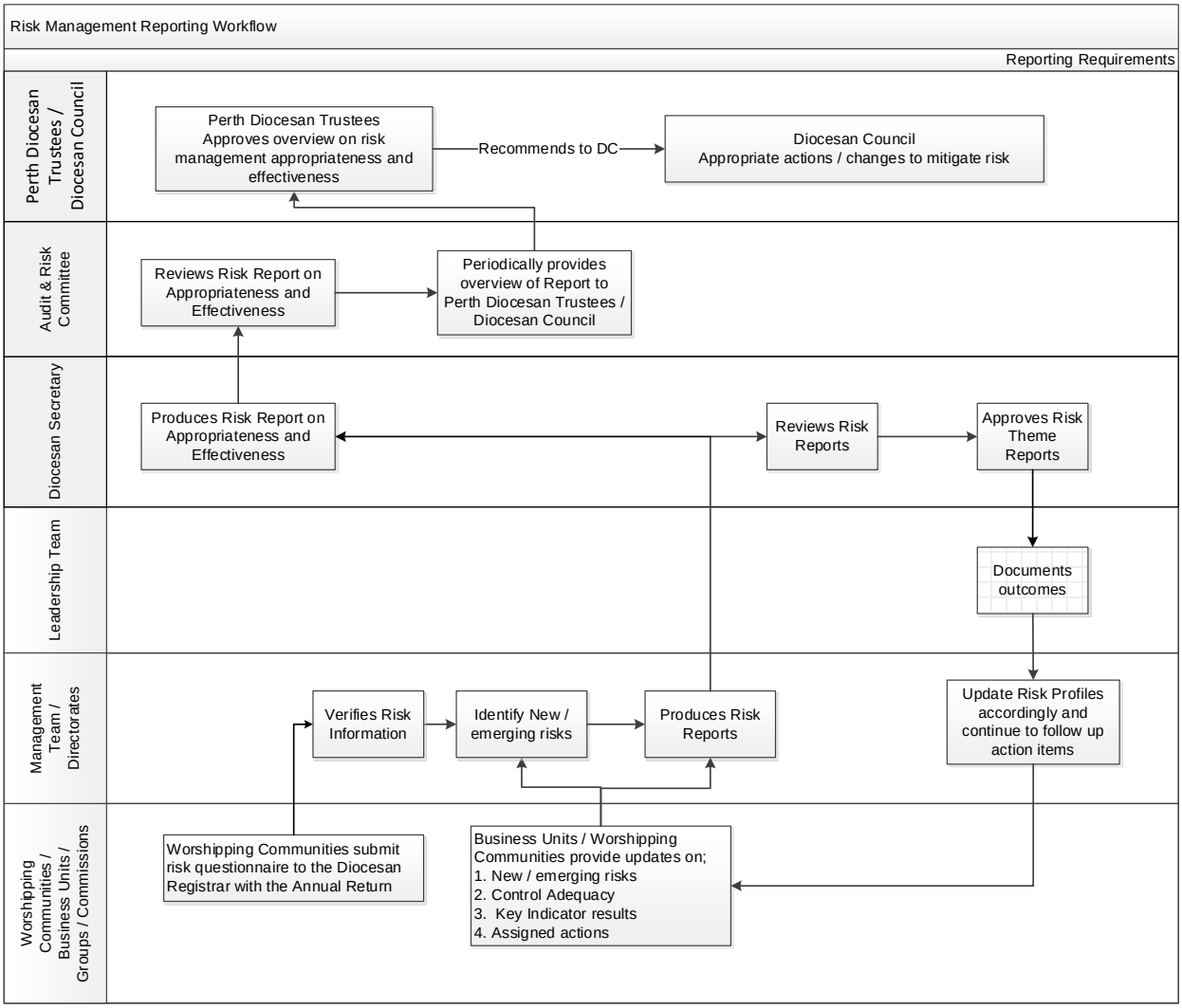

Diagram 4: Risk Management Reporting Process

Each Business Unit / Worshipping Community is responsible for ensuring:

- That their Risk Profiles are formally reviewed and updated, at least on an annual basis or when there has been a material restructure, change in risk ownership or change in the external environment.
- Risks reported to Management are reflective of the current risk and control environment.

Key Indicators

Key Indicators (KI's) are required to be used for monitoring and validating key risks and controls. The following describes the process for the creation and reporting of KIs:

- Identification
- Validity of Source
- Tolerances
- Monitor & Review

Identification

The following represent the minimum standards when identifying appropriate KI's for key risks and controls:

- The risk description and casual factors are fully understood
- The KI is fully relevant to the risk or control
- Predictive KI's are adopted wherever possible
- KI's provide adequate coverage over monitoring key risks and controls

Validity of Source

In all cases an assessment of the data quality, integrity and frequency must be completed to ensure that the KI data is relevant to the risk or Control.

Where possible the source of the data (data owner) should be independent to the risk owner. Overlapping KI's can be used to provide a level of assurance on data integrity.

If the data or source changes during the life of the KI, the data is required to be revalidated to ensure reporting of the KI against a consistent baseline.

Tolerances

Tolerances are set based on the Anglican Church Diocese of Perth Risk Appetite. They are set and agreed over four levels:

- Green – within appetite; no action required.
- Yellow – The KI must be monitored and relevant actions set and implemented to bring the measure back within the green tolerance.
- Amber – the KI must be closely monitored and relevant actions set and implemented to bring the measure back within the green tolerance.
- Red – outside risk appetite; the KI must be escalated to the Senior Management Team where appropriate management actions are to be set and implemented to bring the measure back within appetite.

Monitor & Review

All active KI's are updated as per their stated frequency of the data source.

When monitoring and reviewing KI's, the overall trend must be considered over a longer timeframe instead of individual data movements. The trend of the KI is specifically used as an input to the risk and control assessment.

Appendix A – Risk Assessment and Acceptance Criteria

EXISTING CONTROLS RATING

LEVEL	RATING	FORESEEABLE	DESCRIPTION
E	**Excellent**	Doing more than what is reasonable under the circumstances	Existing controls exceed current legislated, regulatory and compliance requirements, and surpass relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation
A	**Adequate**	Doing what is reasonable under the circumstances	Existing controls are in accordance with current legislated, regulatory and compliance requirements, and are aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation
I	**Inadequate**	Not doing some or all things reasonable under the circumstances	Existing controls do not provide confidence that they meet current legislated, regulatory and compliance requirements, and may not be aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation

MEASURES OF CONSEQUENCE

LEVEL	1	2	3	4	5
RATING	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
PEOPLE	Negligible injuries	First aid injuries	Medical type injuries or Lost time injury < 5 days	Lost time injury > 5 days	Fatality, permanent disability
FINANCIAL	Less than $5,000	$5,000 - $50,000	$50,000 - $2M	$2M - $20M	More than $20M
OPERATIONS	No material service interruption	Temporary interruption to an activity – backlog cleared with existing resources	Interruption to Service Unit/(s) deliverables – backlog cleared by additional resources	Prolonged interruption of critical core service deliverables – additional resources; performance affected	Indeterminate prolonged interruption of critical core service deliverables – non-performance
REPUTATION	Unsubstantiated, localised low impact on key stakeholder trust, low profile or no media item	Substantiated, localised impact on key stakeholder trust or low media item	Substantiated, public embarrassment, moderate impact on key stakeholder trust or moderate media profile	Substantiated, public embarrassment, widespread high impact on key stakeholder trust, high media profile, third party actions	Substantiated, public embarrassment, widespread loss of key stakeholder trust, high widespread multiple media profile, third party actions
LEGAL / COMPLIANCE	Occasional noticeable temporary non-compliances	Regular noticeable temporary non-compliances	Non-compliance with significant regulatory requirements imposed	Non-compliance results in termination of services or imposed penalties	Non-compliance results in criminal charges or significant damages or penalties

MEASURES OF LIKELIHOOD

LEVEL	RATING	DESCRIPTION	FREQUENCY
5	Almost Certain	The event is expected to occur in most circumstances	More than once per year
4	Likely	The event will probably occur in most circumstances	At least once per year
3	Possible	The event should occur at some time	At least once in 3 years
2	Unlikely	The event could occur at some time	At least once in 10 years
1	Rare	The event may only occur in exceptional circumstances	Less than once in 15 years

RISK MATRIX

CONSEQUENCE / LIKELIHOOD		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
Almost Certain	5	MEDIUM (5)	HIGH (10)	HIGH (15)	EXTREME (20)	EXTREME (25)
Likely	4	LOW (4)	MEDIUM (8)	HIGH (12)	HIGH (16)	EXTREME (20)
Possible	3	LOW (3)	MEDIUM (6)	MEDIUM (9)	HIGH (12)	HIGH (15)
Unlikely	2	LOW (2)	LOW (4)	MEDIUM (6)	MEDIUM (8)	HIGH (10)
Rare	1	LOW (1)	LOW (2)	LOW (3)	LOW (4)	MEDIUM (5)

RISK ACCEPTANCE CRITERIA

RISK RANK	LEVEL OF RISK	DESCRIPTION	CRITERIA FOR RISK ACCEPTANCE	RESPONSIBILITY
EXTREME	17 – 25	Urgent Attention Required	Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	Executive Officer / Trustees
HIGH	10 – 16	Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Director / Executive Officer
MEDIUM	5 – 9	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Manager / Director
LOW	1 – 4	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Warden / Supervisor

Appendix B – Risk Theme Definitions

1) Key Stakeholder Relationships

Failure to provide or be provided with agreed and/or expected levels of service and engagement to/from key internal or external stakeholders impacting the deliverables of the Church and/or Diocese

2) Unsustainable / Inefficient Practices & Operations

The difficulties of operating a commercial, sustainable business model within the Church hierarchy, governance framework and historical legacy

3) Safety & Health

Inadequate safety and health policy, framework, systems and structures to prevent injury to clergy, staff, volunteers, contractors, parishioners and/or visitors in the provision of a working environment or church activities. Includes subsequent public liability and workers compensation claims due to personal harm

4) Statutory, Regulatory & Compliance

Failure to correctly identify, interpret, assess, respond, communicate and comply with legislation, statutes and policies

5) Fraud & Misconduct

Intentional activities in excess of authority granted to an office holder or employee, which circumvent endorsed statutes, policies, procedures or delegated authority

6) Service / Business Interruption

An event causing the inability to continue Church activities and/or Diocese functions

7) Commercial Development

Failure to effectively manage costs, controls and critical dependencies associated with commercial property development

8) Commercial Asset Management

Failure to effectively manage the day to day operations of commercial properties including user/tenant agreements, maintenance and inspection programmes and procedures in place to manage quality, usage and availability

9) Parish Property Management

Failure to effectively manage the day to day operations of parish properties including user/tenant agreements, maintenance and inspection programmes and procedures in place to manage quality, usage and availability

10) Professional Standards

Failure to implement, update, renew, communicate and monitor effectiveness of professional standards measures to protect vulnerable members of the Church community. Includes subsequent liability and compensation claims.

Appendix A - Risk Assessment and Acceptance Criteria

EXISTING CONTROLS RATING

LEVEL	RATING	FORESEEABLE	DESCRIPTION
E	**Excellent**	Doing more than what is reasonable under the circumstances	Existing controls exceed current legislated, regulatory and compliance requirements, and surpass relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation
A	**Adequate**	Doing what is reasonable under the circumstances	Existing controls are in accordance with current legislated, regulatory and compliance requirements, and are aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation
I	**Inadequate**	Not doing some or all things reasonable under the circumstances	Existing controls do not provide confidence that they meet current legislated, regulatory and compliance requirements, and may not be aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation

MEASURES OF CONSEQUENCE

LEVEL	1	2	3	4	5
RATING	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
PEOPLE	Negligible injuries	First aid injuries	Medical type injuries or Lost time injury < 5 days	Lost time injury > 5 days	Fatality, permanent disability
FINANCIAL	Less than $5,000	$5,000 - $50,000	$50,000 - $2M	$2M - $20M	More than $20M
OPERATIONS	No material service interruption	Temporary interruption to an activity – backlog cleared with existing resources	Interruption to Service Unit/(s) deliverables – backlog cleared by additional resources	Prolonged interruption of critical core service deliverables – additional resources; performance affected	Indeterminate prolonged interruption of critical core service deliverables – non-performance
REPUTATION	Unsubstantiated, localised low impact on key stakeholder trust, low profile or no media item	Substantiated, localised impact on key stakeholder trust or low media item	Substantiated, public embarrassment, moderate impact on key stakeholder trust or moderate media profile	Substantiated, public embarrassment, widespread high impact on key stakeholder trust, high media profile, third party actions	Substantiated, public embarrassment, widespread loss of key stakeholder trust, high widespread multiple media profile, third party actions
LEGAL / COMPLIANCE	Occasional noticeable temporary non-compliances	Regular noticeable temporary non-compliances	Non-compliance with significant regulatory requirements imposed	Non-compliance results in termination of services or imposed penalties	Non-compliance results in criminal charges or significant damages or penalties

MEASURES OF LIKELIHOOD

LEVEL	RATING	DESCRIPTION	FREQUENCY
5	**Almost Certain**	The event is expected to occur in most circumstances	More than once per year
4	**Likely**	The event will probably occur in most circumstances	At least once per year
3	**Possible**	The event should occur at some time	At least once in 3 years
2	**Unlikely**	The event could occur at some time	At least once in 10 years
1	**Rare**	The event may only occur in exceptional circumstances	Less than once in 15 years

RISK MATRIX

CONSEQUENCE / LIKELIHOOD		Negligible	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
Almost Certain	5	MEDIUM (5)	HIGH (10)	HIGH (15)	EXTREME (20)	EXTREME (25)
Likely	4	LOW (4)	MEDIUM (8)	HIGH (12)	HIGH (16)	EXTREME (20)
Possible	3	LOW (3)	MEDIUM (6)	MEDIUM (9)	HIGH (12)	HIGH (15)
Unlikely	2	LOW (2)	LOW (4)	MEDIUM (6)	MEDIUM (8)	HIGH (10)
Rare	1	LOW (1)	LOW (2)	LOW (3)	LOW (4)	MEDIUM (5)

RISK ACCEPTANCE CRITERIA

RISK RANK	LEVEL OF RISK	DESCRIPTION	CRITERIA FOR RISK ACCEPTANCE	RESPONSIBILITY
EXTREME	**17 – 25**	Urgent Attention Required	Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	Executive Officer / Trustees
HIGH	**10 – 16**	Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Director / Executive Officer
MEDIUM	**5 – 9**	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Manager / Director
LOW	**1 – 4**	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Warden / Supervisor

Appendix B – Risk Theme Definitions

1) Key Stakeholder Relationships

Failure to provide or be provided with agreed and/or expected levels of service and engagement to/from key internal or external stakeholders impacting the deliverables of the Church and/or Diocese

2) Unsustainable / Inefficient Practices & Operations

The difficulties of operating a commercial, sustainable business model within the Church hierarchy, governance framework and historical legacy

3) Safety & Health

Inadequate safety and health policy, framework, systems and structures to prevent injury to clergy, staff, volunteers, contractors, parishioners and/or visitors in the provision of a working environment or church activities. Includes subsequent public liability and workers compensation claims due to personal harm

4) Statutory, Regulatory & Compliance

Failure to correctly identify, interpret, assess, respond, communicate and comply with legislation, statutes and policies

5) Fraud & Misconduct

Intentional activities in excess of authority granted to an office holder or employee, which circumvent endorsed statutes, policies, procedures or delegated authority

6) Service / Business Interruption

An event causing the inability to continue Church activities and/or Diocese functions

7) Commercial Development

Failure to effectively manage costs, controls and critical dependencies associated with commercial property development

8) Commercial Asset Management

Failure to effectively manage the day to day operations of commercial properties including user/tenant agreements, maintenance and inspection programmes and procedures in place to manage quality, usage and availability

9) Parish Property Management

Failure to effectively manage the day to day operations of parish properties including user/tenant agreements, maintenance and inspection programmes and procedures in place to manage quality, usage and availability

10) Professional Standards

Failure to implement, update, renew, communicate and monitor effectiveness of professional standards measures to protect vulnerable members of the Church community. Includes subsequent liability and compensation claims.