



RISK MANAGEMENT

Recommended by PDT Audit and Risk Committee
Approved by the Perth Diocesan Trustees
Approved by Diocesan Council

28 November 2023
7 December 2023
15 February 2024

Contents

PART 1 - POLICY	3
1. Preamble	3
2. Scope	3
3. Statement of Objectives	3
4. Risk Appetite Statement	3
5. Risk Culture Statement	4
6. Risk Management Process Statement	4
7. Context	4
8. Roles and Responsibilities	4
PART 2 - RISK FRAMEWORK	6
1. Introduction	6
2. Alignment with Risk Appetite Statement	6
3. Alignment with Risk Culture Statement	6
4. Roles and Responsibilities	7
5. Risk Management Process	8
5.1 Communications and Consultation	8
5.2 Scope, Context and Criteria	9
5.3 Risk Assessment	10
5.4 Risk Treatment	11
5.5 Monitoring and Review	12
5.6 Recording and Reporting	12
Appendix A – Risk Management Glossary	14
Appendix B – Summary of Key Risk Management Activities	16
Appendix C – Risk Escalation Criteria	18

**DIOCESAN COUNCIL /
THE PERTH DIOCESAN TRUSTEES
POLICY 41**

**Anglican
Church**
Diocese of Perth



Appendix D – Risk Escalation Process	19
Appendix E – Risk Treatment Plan Template	20
Appendix F – Risk Management Communication Strategy.....	21
Appendix G – Risk Register Template	24
Appendix H – Risk Theme Definitions	25
Appendix I – Controls Effectiveness Rating.....	26
Appendix J - Likelihood Criteria.....	27
Appendix K – Consequence Criteria.....	28
Appendix L – Risk Rating Matrix.....	31



PART 1 - POLICY

1. Preamble

- 1.1 The Anglican Diocese of Perth (ADP) is committed to maintaining an organisation-wide Risk Management Policy and Framework (the framework) to support good governance, sound decision making and improved performance for both ministry and business outcomes. It helps to achieve objectives, improve performance, prevent harm and promote resilience.
- 1.2 The framework (detailed in Part 2) is aligned with better practice guidelines and standards, in particular the Australian and New Zealand Standard AS/NZS ISO 31000 – Risk Management Guidelines.

2. Scope

- 2.1 This policy applies to all ADP sites, including but not limited to; all parishes, St George's Cathedral, Diocesan Office, Swan Valley Adventure Centre (SVAC), Wollaston Theological College (WTC) and commercial property assets.
- 2.2 This policy applies to all ADP members, including but not limited to; the Episcopate, the Perth Diocesan Trustees (PDT), Diocesan Council (DC), lay and operational employees, clergy, parish office bearers and parish councillors.

3. Statement of Objectives

- 3.1 The ADP's strategy and risk objectives form the reference point for its risk appetite. The ADP risk objectives are:
 - a. Protect people and property from harm and damage.
 - b. Prevent financial loss and enhance investment returns within risk appetite.
 - c. Enhance organisational resilience and provide for the continuity of critical mission and business operations.
 - d. Protect our reputation and reassure stakeholders.
 - e. Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.
 - f. Provide transparent and formal oversight of the risk environment, to enable effective decision making and efficient use of resources.

4. Risk Appetite Statement

- 4.1 The Risk Appetite Statement sets out the amount and type of risks the ADP is able and willing to accept in order to achieve its strategic objectives.
- 4.2 In understanding the history of the Church and the ADP, and the legacy of those that have gone before us, the PDT and DC recognise their responsibility to preserve our heritage for future generations. In view of this, the following defines the ADP appetite for risk:
 - a. Risks to people, ministry and business operations, reputation and legal compliance are to be managed as low as reasonably practical.
 - b. Risk to financial investments are to be managed in accordance with Policy 25 – PDT Investments, which states: "The PDT have a policy of investing all funds available for investment for maximum return while recognising their obligations to manage an investment portfolio in such a manner



that will achieve a reasonable balance between investment return and security over the investment assets under their control.”

5. Risk Culture Statement

- 5.1 Risk Culture refers to the behaviours that lead to how everyone thinks about and manages risk. It is part of the overall culture of our organisation.
- 5.2 The PDT, DC, Archbishop and Diocesan Secretary are responsible for setting the “tone at the top” and play a key role in influencing a role modelling a positive risk culture.
- 5.3 Our behaviours should be driven by Christian principles and Anglican traditions, which underpin the way we treat people and steward resources.
- 5.4 Risk management is everyone’s responsibility.

6. Risk Management Process Statement

- 6.1 Risk management processes must be detailed enough to provide a true assessment of risk, be flexible enough to respond to changing circumstances and deliver the capacity to identify new or emerging risks.
- 6.2 Risk reporting must be sufficiently detailed and accurate to enable to PDT and DC to fulfil their positive duty requirements under legislation.

7. Context

- 7.1 This policy should be read in conjunction with:
 - a. *ADP Mission and Values*
 - b. *Diocesan Trustees Statute 2016*
 - c. *Parish Governance Statute 2017*
 - d. *Policy 46 - DC Governance*
 - e. *Policy 46.1 - PDT Governance*
 - f. *Policy 25 - PDT Investments*
 - g. *Policy 22 – PDT Audit and Risk Committee Charter*
 - h. *Diocesan Website Risk Management resources*

8. Roles and Responsibilities

- 8.1 The following details set out clear accountability and responsibilities for Committees and the Diocesan Secretary:
 - 8.1.1 **The Perth Diocesan Trustees** are accountable for:
 - a. Approving the Risk Management Policy from an employer, land and asset owner, financial, business operations, business reputation and legal perspective.
 - b. Appointing the PDT Audit and Risk Committee and providing their terms of reference.
 - c. Receiving risk management reports and assess the effectiveness of risk identification, assessment, control and monitoring against the relevant business and risk objectives.
 - d. Driving a positive risk culture in Diocesan Office and business-related entities.
 - e. Developing policies, which effectively control risk.



- f. Directing the renewal of insurance policies as required.

8.1.2 **Diocesan Council** is accountable for:

- a. Approving the Risk Management Policy from a mission, ministry operations, ministry reputation and parish perspective.
- b. Appointing the DC Risk Committee and provide their terms of reference.
- c. Receiving risk management reports and assess the effectiveness of risk identification, assessment, control and monitoring against the relevant ministry and risk objectives.
- d. Driving a positive risk culture in Episcopal Office, parishes and other ministry related entities.
- e. Developing statutes and policies, which effectively control risk.

8.1.3 The **PDT Audit and Risk Committee** is responsible for:

- a. Oversight of the risk management policy and framework.
- b. Advising the PDT on emerging risks and variation in existing risks.
- c. Monitoring compliance with risk appetite.
- d. Reviewing risk information, including trends and themes from incidents and events to report to the PDT.
- e. Liaising with external auditors and monitoring corrective actions.
- f. Ensuring relevant information from other subcommittees is provided to inform the progress of key strategic business risks.

8.1.4 The **DC Risk Committee** is responsible for:

- a. Advising DC on emerging ministry risks and variation in existing risks.
- b. Advising DC on a positive risk culture in Episcopal Office, parishes and other ministry related entities.
- c. Reviewing risk information, including trends and themes from incidents and events to report to the DC.

8.1.5 The **Diocesan Secretary** is responsible for organisational leadership of the risk framework:

- a. Fosters a positive risk-aware culture across the organisation.
- b. Ensures risk framework is integrated into strategic, operational and project management.
- c. Establishes risk reporting and communication framework and monitors key risk information.
- d. Oversees communication to Risk Committees, the PDT and DC on risk management and compliance with risk appetite.
- e. Ensures staff understand their risk management role and incorporates this in performance reviews.
- f. Provides resources to build risk capabilities across the organisation.
- g. Establishes strategic risk profile and ensures it is reviewed in accordance with PDT and DC expectations.
- h. Support the internal audit program and ensure all corrective actions are addressed.
- i. Supports the review of the risk management framework, at least every three years.



PART 2 - RISK FRAMEWORK

1. Introduction

- 1.1 The framework provides details on how we will deliver the requirements of the:
 - a. Risk Appetite Statement at Part 1 Section 4,
 - b. Risk Culture Statement at Part 1 Section 5, and
 - c. Risk Management Process Statement at Part 1 Section 6.
- 1.2 The framework may be updated from time to time by the Diocesan Secretary, particularly in regard to changes in AS/NZS ISO 31000 – Risk Management Guidelines. The Appendices form part of the framework.
- 1.3 The following appendices will assist in understanding:
 - a. *Appendix A – Risk Management Glossary*
 - b. *Appendix B – Summary of Key Risk Management Activities*

2. Alignment with Risk Appetite Statement

- 2.1 To ensure risk appetite requirements are met, for any risks rated HIGH or EXTREME, the following is required:
 - a. Risk escalation in accordance with:
 - o *Appendix C – Risk Escalation Criteria* and,
 - o *Appendix D – Risk Escalation Process*.
 - b. Risk treatment in accordance with:
 - o *Appendix E – Risk Treatment Plan Template*.
- 2.2 In addition, risks rated HIGH are to be reported to the PDT and DC every six months and risks rated EXTREME at every PDT and DC meeting.

3. Alignment with Risk Culture Statement

- 3.1 Appropriate behaviours are communicated in our mission, in statutes and policies, the diocesan website and face to face training.
- 3.2 Risk Treatment Controls should be embedded in position descriptions.
- 3.3 Risk management should be a component of performance assessment.
- 3.4 Regular internal and external communication and consultation in line with section 4.1 below is essential.
- 3.5 Key training courses (e.g., Safe Ministry and WHS) should include appropriate risk management guidance.
- 3.6 Our risk culture is measured through the grievance and complaints reporting process, work health and safety reports, safeguarding and financial indicators.



4. Roles and Responsibilities

- 4.1 In addition to the roles and responsibilities in Part 1 Section 8, the following details the role and responsibilities of Senior Management, Risk and Treatment Owners:
- 4.1.1 The **Senior Clerical and Diocesan Staff** (Assistant Bishops, Dean, Archdeacons, Diocesan Operations Manager, Diocesan Property Services Manager, Diocesan Human Resources Manager, Safe Ministry Services Manager, General Manager – SVAC and the Principal of the Theological College) are responsible for assisting the bodies and officers in part 1 Section 8 by:
- a. Integrate risk management in strategic and operational planning.
 - b. Ensure risk framework is integrated with regulatory and organisational frameworks.
 - c. Monitor and review risks and risk-related information (incidents, complaints, serious events) and escalate as required.
 - d. Ensure staff are orientated to the risk framework and education programs are in place to support risk capabilities.
 - e. Identify new and emerging risks and the relevant risk owners.
 - f. Provide resources for staff to manage risks.
 - g. Monitor and report to Diocesan Secretary on risk culture.
- 4.1.2 In addition to the above, the **Diocesan Operations Manager** is responsible to coordinate the implementation and ongoing development of risk management across the organisation:
- a. Support staff to understand their responsibilities with respect to risk management and are provide training, education and assistance.
 - b. Support the executive with the management of the strategic risk register and reporting.
 - c. Support activities and priorities of the internal audit function.
 - d. Monitor and coordinate reviews and continuous improvement of the framework and risk culture.
 - e. Monitor compliance with regulatory obligations.
- 4.1.3 The **Risk Owner** is a person or entity with accountability for:
- a. Monitoring the assigned risk.
 - b. Understanding the scope and context of the risk.
 - c. Assigning risk control owners.
 - d. Assisting in developing risk control plans.
 - e. Executing those plans if necessary.
 - f. Collaborating with other team members on risk control.
 - g. Identifying, assessing, monitoring, and managing potential threats and sub-risks.
 - h. Determining the appropriate risk rating.
 - i. Determining appropriate control effectiveness rating.
 - j. Integrating risk management into operational activities.
 - k. Remediating gaps in control and monitoring activities.
- 4.1.4 The **Risk Control Owner** is a person or entity with accountability for:
- a. Understand the scope of the risk and how the control is crucial to preventing or mitigation failure.
 - b. The design of the control and what is required to make it work effectively.
 - c. Conduct control effectiveness assessments.
 - d. Update the risk owner as required.
- 4.1.5 The **Risk Treatment Owner** is the person accountable for monitoring and reporting implementation progress of the treatment plan.

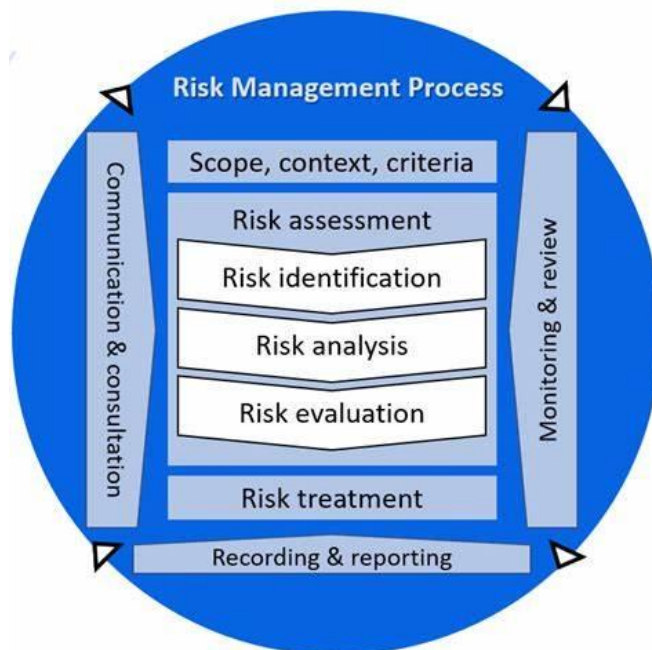


- 4.1.6 **Clergy, employees and parish office bearers** are responsible for:
- a. Promote and support a positive risk culture across the organisation.
 - b. Adhere to risk management policy and framework.
 - c. Participate in the identification and management of risks relevant to roles and responsibilities.
 - d. Report new or emerging risks to line manager.
 - e. Report and manage incidents, complaints and hazards in a timely way to line manager.

5. Risk Management Process

The Risk Management process has six key stages:

- a. **Communication and Consultation** - with internal and external stakeholders.
- b. **Scope, Context and Criteria** - the boundaries.
- c. **Risk Assessment** – risk identification, analysis and evaluation.
- d. **Risk Treatment** – implement and assess actions to address risk.
- e. **Monitoring and Review** – risk reviews and audit.
- f. **Recording and Reporting** – what needs to be documented and reported.



5.1 Communications and Consultation

- 5.1.1 The ADP communicates with both internal and external stakeholders, with roles and responsibilities in managing risk or with an interest in an outcome.
- 5.1.2 **Internal Communication and Consultation**
- 5.1.3 Communication and consultation internally builds a risk aware workforce and supports accountability and ownership of risk. This includes:
- a. avenues to support the flow of information through the organisation,
 - b. avenues to facilitate consultation through the organisation
 - c. education and training around the principles of risk management, and



- d. the provision of tools and resources to manage risk.

5.1.4 This is achieved through:

- a. Synod sessions,
- b. PDT and DC meetings,
- c. Archbishop's Leadership Forum meetings,
- d. Deanery meetings,
- e. Parish Council meetings,
- f. Diocesan Office Management Team meetings,
- g. Parish Office Bearer workshops,
- h. Diocesan Office advice and support, and
- i. Diocesan Website internal resources.

5.1.5 **External Communication and Consultation**

5.1.6 Communication and consultation with external stakeholders supports effective exchange of risk information and helps build confidence in the organisation's management. This includes:

- a. external reporting to meet regulatory, governance and compliance requirements;
- b. communication with clients and stakeholders in the event of major or incident a crisis; and,
- c. communication with stakeholders and third parties on the management of risk.

5.1.7 This is achieved through:

- a. reports to General Synod,
- b. reports to Diocesan Synod,
- c. reports to the PDT and DC,
- d. statutory reports,
- e. external audits,
- f. insurance disclosure information, and
- g. Diocesan Website public information.

Also see [Appendix F – Risk Management Communication Strategy](#).

5.2 **Scope, Context and Criteria**

5.2.1 Establishing the scope, context and criteria defines the basic parameters for managing risks. This includes considering the external environment and stakeholders, the internal environment and our appetite for risk:

EXTERNAL ENVIRONMENT	Social factors, community expectations, demographics, networks and dependencies, market trends and emerging risks.
EXTERNAL STAKEHOLDERS	Insurers, service clients, service providers, regulators and parishioners.
INTERNAL ENVIRONMENT	Objectives, culture, vision, mission and values, strategy, governance and organisational structures, systems, processes, standards, key performance indicators and other drivers.
APPETITE FOR RISK	What risks do we want to take and how much?



- 5.3.2 Primarily our context is driven by being a Christian organisation, where coming to church or being part of a worshipping community is very much a choice. Effectively managing risk will have a positive influence on this choice.

5.3 Risk Assessment

- 5.3.1 Risk Assessment is documented using [Appendix G – Risk Register Template](#).
- 5.3.2 To aid assessment risk are grouped under themes using [Appendix H – Risk Theme Definitions](#).
- 5.3.3 The risk assessment process includes identifying, analysing and evaluating the risk and is documented in the Risk Register. Risks are always assessed against mission and, ministry, business and risk objectives.
- 5.3.4 **Risk Identification**
- 5.3.5 Risk identification is the process of identifying, recognising and recording the organisations risks. The purpose of risk identification is to identify what might happen or situations that might exist that may affect the achievement of the ADP’s objectives.
- 5.3.6 It involves deliberately stopping to think about:
- What **event** could occur and what are the **potential threats** or **risk** that may cause this?
 - What is the **impact** or **consequences** for the organisation?
- 5.3.7 The key questions when identifying risks are:
- What** can happen?
 - Where** can it happen?
 - When** can it happen?
 - Why** can it happen?
 - How** can it happen?
 - What** is the impact?
 - Who** is responsible for managing the risk?
- 5.3.8 A risk is the “effect of uncertainty on objectives” and is expressed in terms of the likelihood of an event occurring and consequence of that event. There are three types of risks:

STRATEGIC RISKS	Managed by the PDT, DC and Diocesan Secretary. Detailed in the PDT and DC Risk Registers.
OPERATIONAL RISKS	Managed by Business (e.g., SVAC and WTC) Unit Managers. Managed by Parish Councils.
PROJECT RISKS	Managed by Commercial Asset Managers or Project Manager. Details in Project Risk Register.

- 5.3.9 Considerable effort needs to be given to emerging risk, as these can creep up on us if there is not a deliberate effort to consider alternate futures.
- 5.3.10 **Risk Analysis**
- 5.3.11 Risk analysis assists to:
- Identify effects on the organisation of the risk.
 - Assess current controls, their effectiveness and determine gaps.
 - Determine the severity or level of risk (risk rating) to objectives.
 - Assess and strengthen risk controls.



- 5.3.12 Risk Controls are tasks which actively change the likelihood of a risk occurring. These can be supported by policies, procedures, systems and training to know what to do and when. They can also be manual or automated in nature.
- 5.3.13 A key control is a control which significantly alters the likelihood or consequence of the risk event, often acting independently from other controls. There are two types of controls:
- Preventative Controls** – aimed at preventing the risk occurring in the first place or reducing the likelihood of the event occurring. They include policies and procedures, training and systems. A variation on this is detective controls used to identify when a risk has become an issue/incident. They include audits, reviews, etc.
 - Mitigating Controls** – aimed at reducing the consequences that comes from the issue/incident. They may include the provision of first aid or counselling, insurance, business continuity plans, engaging consultants to assist in reputation damage or legal advice.
- 5.3.14 Steps for analysing risks.
- What is currently in place to manage the risk?
 - How effective are these measures? ([Appendix I – Controls Effectiveness Rating](#))
 - What is the likelihood of the risk occurring? ([Appendix J - Likelihood Criteria](#))
 - What are the potential consequences should the risk occur? ([Appendix K – Consequence Criteria](#)).
 - Based on the combination of likelihood and consequences what is the level of risk? ([Appendix L – Risk Rating Matrix](#))
- 5.3.15 **Risk Evaluation**
- 5.3.16 Based on the risk analysis and the resultant Risk Rating, the next step in the process is to determine which risks require further action and the priority for implementing the response.
- 5.3.17 Risk evaluation assists to:
- escalate risk information to the necessary reporting levels,
 - prioritise risks,
 - identify options and choose required actions, and
 - identify resources required.
- 5.4 Risk Treatment**
- 5.4.1 A risk treatment plan is the process of selecting one or more options for mitigating risks and implementing those options. The treatment plan owner is the person accountable for monitoring and reporting implementation progress of the treatment plan. The treatment plan owner is supervised by the risk owner, or it may be the same person.
- 5.4.2 All HIGH and EXTREME risks should be reported to the PDT and DC every six months and have a Risk Treatment Plan developed.
- 5.4.3 Risk treatment involves:
- identifying options for controlling the risk, and
 - designing and implementing a treatment plan.
- 5.4.4 The following options are available for controlling the risk:
- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk,
 - removing the risk source,
 - changing the likelihood,



- d. changing the consequences, and
- e. sharing the risk with another party or parties (including insurers).

5.4.5 The information provided in a risk treatment plan should include:

- a. the reasons for selection of treatment options, including expected benefits;
- b. those accountable for approving and responsible for implementing the plan;
- c. proposed actions;
- d. resource requirements;
- e. the order in which actions / tasks should be completed;
- f. monitoring and communication plan; and,
- g. timeframe for completing deliverables.

5.5 Monitoring and Review

- 5.5.1 Risks will be continuously monitored and reviewed and the effectiveness of the controls in place will be assessed to ensure changing circumstances do not alter risk priorities.
- 5.5.2 Feedback on the effectiveness of the Risk Management Policy and Framework will be obtained from the risk reporting process and other available information, including:
 - a. annual parish returns,
 - b. annual financial audits,
 - c. six- and twelve-monthly mandatory test and compliance inspections,
 - d. three yearly maintenance and structural assessments, and
 - e. safe ministry checks.
- 5.5.3 Risks and controls will be monitored and tested regularly through continuous improvement programs.

5.6 Recording and Reporting

- 5.6.1 Risk reporting is an important way of communicating risk information throughout the ADP. Risks should be logged and monitored using the Risk Register.
- 5.6.2 The ADP has the following reporting and reporting structures:
 - a. The PDT will receive a Risk Report on one or two risk themes at every meeting, plus the treatment plans developed for any HIGH or EXTREME risks.
 - b. DC will receive a Risk Report at every meeting which will cover one or two risk themes.
 - c. The PDT Audit and Risk Committee will receive an annual report with a policy review, summary of all risks, a summary of control improvements and advice on emerging risks.
 - d. The Diocesan Office Management Team will meet annually to review the PDT and DC Risk Register.
 - e. The SVAC Risk Management Committee will meet quarterly to review the SVAC Risk Register.
 - f. Incident and Hazard reports will be raised as required and provided to the PDT and DC in the WHS Report at every meeting.
 - g. Risk Owners will escalate risk as required if circumstances change.
 - h. External reviews.

DIOCESAN COUNCIL / THE PERTH DIOCESAN TRUSTEES POLICY 41

**Anglican
Church**
Diocese of Perth



5.6.3 The table below summarises the risk reporting requirements:

REPORT	FREQUENCY	AUDIENCE
PDT STRATEGIC RISK REPORT	Six times per year	PDT
DC STRATEGIC RISK REPORT	Six times per year	DC
ANNUAL POLICY AND EMERGING RISK REVIEW	Annual	PDT A&RC
SENIOR MANAGEMENT TEAM RISK REVIEW	Annual	Diocesan Secretary
RISK TREATMENT PLANS	As Required	Diocesan Secretary PDT and DC
SVAC OPERATIONAL RISK REVIEW	Quarterly	Operations Manager
COMMERCIAL BUILDING WHS REPORTS	Six monthly	Operations Manager
INTERNAL AUDIT REPORT	As required	Relevant Manager
EXTERNAL AUDITS REPORTS	Annual	Relevant Manager
INCIDENT AND HAZARD REPORTS	On Occurrence	Operations Manager

5.6.4 Risk owners will monitor the currency and status of the risks allocated to them. Risks are to be formally monitored and reviewed/reported on by the risk owner in accordance with the table below:

RISK LEVEL	REPORTING FREQUENCY TO PDT AND DC
EXTREME	Every meeting
HIGH	Every six months
MEDIUM	Annually
LOW	Annually
VERY LOW	Annually



Appendix A – Risk Management Glossary

communication and consultation	processes to provide, share or obtain information and to engage in dialogue with stakeholders and others regarding the management of risk
consequence	outcome of an event affecting objectives
control	measure that is modifying risk
establishing the context	defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy
external context	external environment in which the organisation operates to achieve its objectives
internal context	internal environment in which the organisation seeks to achieve its objectives
level of risk	scale of a risk, expressed in terms of consequences and likelihood
likelihood	chance of something happening
monitoring	continual checking, supervising, observing or determining the status of a risk to identify changes required or expected
risk	effect of uncertainty on objectives
risk analysis	process to understand an organisations risks and to determine the level of risk
risk assessment	process of risk identification, risk analysis and risk evaluation
risk aversion	attitude to turn away from risk
risk criteria	reference against which the impact of a risk is evaluated
risk evaluation	process of comparing of risk analysis with risk criteria to determine whether the risk and/or its impact is acceptable or tolerable
risk identification	process of identifying and describing risks that can and will impact the organisations objectives



risk management framework	components that outline the organisations approach for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
risk management policy	statement of the organisations intentions and direction related to risk management
risk management process	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 owner	person with the responsibility to manage a risk and coordinate the input of others.
risk rating	risk remaining after risk treatment
risk register	description of any set of risks
risk review	activity to determine the suitability, adequacy and effectiveness of risk management framework to achieve established objectives
risk source	Elements that have the potential to give rise to risk event
risk treatment	process to modify risk



Appendix B – Summary of Key Risk Management Activities

ACTION	DESCRIPTION	RESPONSIBILITY	WHEN
Review Risk Management Policy and Framework	Review the effectiveness of ADP's Risk Management Policy and Framework	PDT A&RC Diocesan Secretary Operations Manager	Annually November
Risk Status Report	Review relevant risks, the status of controls and whether the risk rating is with acceptance limits.	PDT and DC Diocesan Secretary Operations Manager	Every meeting
Identify new or emerging risks	Identify new or emerging risks	PDT A&RC Senior Management Team	Annually
Policy Development	Develop policy as an effective preventative risk control	Policy Committee Operations Manager	As required
Training Development	Develop training as an effective preventative risk control	Operations Manager Human Resources Manager	As required
Implement Risk Treatment Plans	Implement actions contained in risk treatment plans	Risk Owner	As required

**DIOCESAN COUNCIL /
THE PERTH DIOCESAN TRUSTEES
POLICY 41**



Clergy and Employee Performance Review	Ensure risk control is assessed in performance reviews.	Managers	Annually
Employee Position Descriptions	Ensure preventative risk controls are built into position descriptions.	Human Resources Manager Line Manager	Annually
Communication	Develop communications channels as an effective risk control.	Diocesan Secretary Operations Manager	As required
Insurance Review	Develop insurance as an effective mitigating risk control.	Diocesan Secretary Chief Financial Officer Operations Manager	Annually August to October

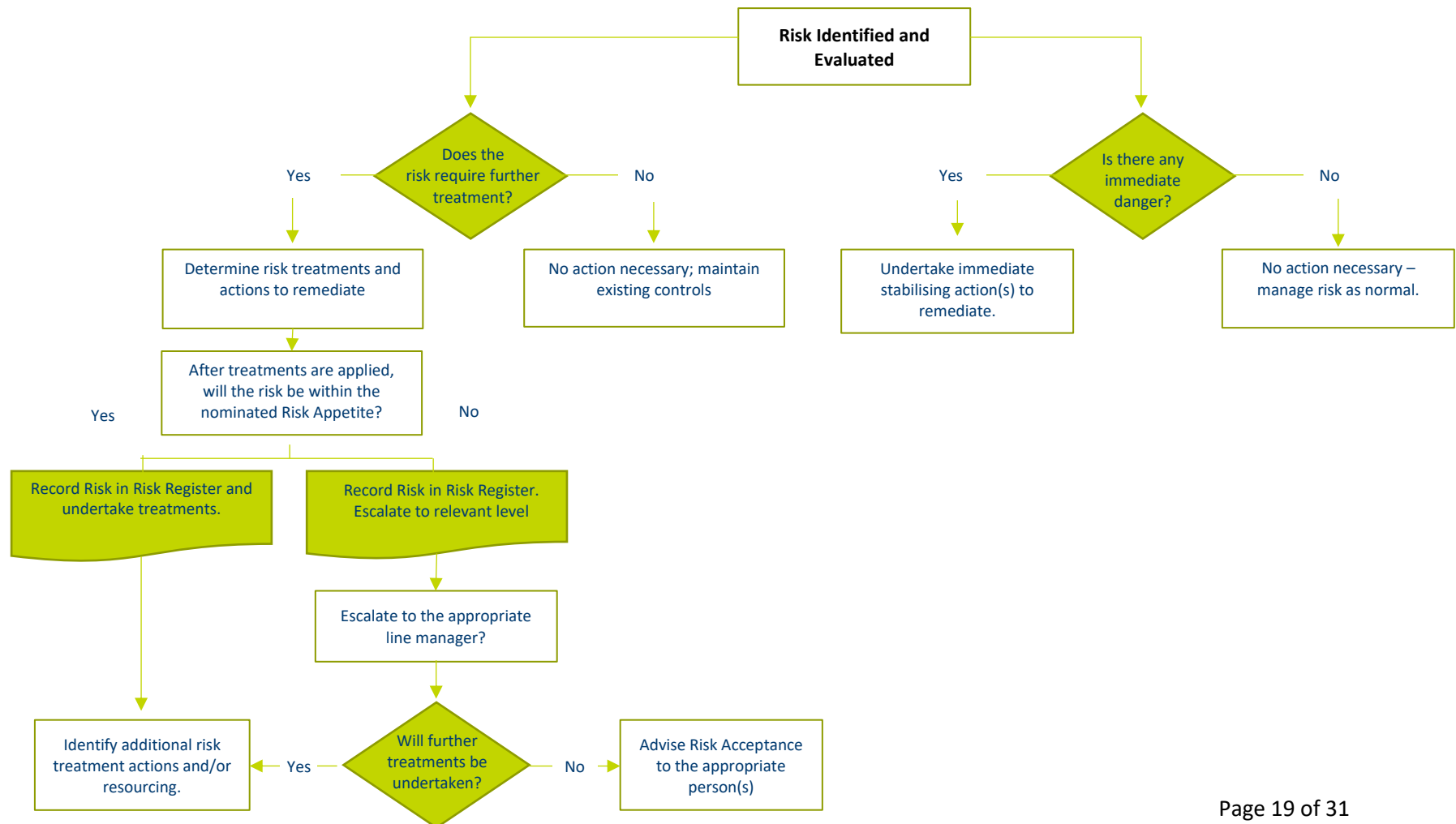


Appendix C – Risk Escalation Criteria

RISK LEVEL	ACTION REQUIRED
EXTREME	<p>Immediate action required.</p> <p>Escalate to Diocesan Secretary, PDT and DC.</p> <p>Risk Treatment Plan to be led by the Senior Management Team and reported to PDT and DC at every meeting.</p>
HIGH	<p>Action required within three months.</p> <p>Escalate to Diocesan Secretary, PDT and DC.</p> <p>Risk Treatment Plan to be led by Risk Owner and Operations Manager and reported to PDT and DC every six months.</p>
MEDIUM	<p>Risk Owner and Operations Manager seek improvement to controls.</p>
LOW	<p>Risk Owner and Operations Manager to monitor.</p>
VERY LOW	<p>Risk Owner and Operations Manager to monitor.</p>



Appendix D – Risk Escalation Process





Appendix E – Risk Treatment Plan Template

RISK	POSSIBLE TREATMENT OPTIONS	PREFERRED OPTIONS	ACCEPT / REJECT OPTION	WHO WILL IMPLEMENT OPTION/S?	BY WHEN?	HOW WILL THE RISK AND TREATMENT OPTION BE MONITORED?



Appendix F – Risk Management Communication Strategy

Internal Stakeholder Communications Plan

STAKEHOLDER NAME	STAKEHOLDER TYPE	DELIVERY METHOD
Synod	Board	Synod Papers
Archbishop	Leadership	Email / Meetings
PDT	Board	PDT Papers
DC	Board	DC paper
PDT A&RC	Committee	PDT A&RC Papers
DC Risk Committee	Committee	DC RC Papers
Episcopal Office	Management Team	Email / Meetings
Diocesan Office	Management Team	Email / Meetings
	Risk Owners	Email
	Risk Treatment Owners	Email
Business Units	Managers	LMS / Email / Meetings
Parishes	Clergy / Parish Office Bearers	LMS / Email / POBW / Website / Deanery meetings / Parish Council meetings

**DIOCESAN COUNCIL /
THE PERTH DIOCESAN TRUSTEES
POLICY 41**

**Anglican
Church**
Diocese of Perth



External Stakeholder Communications Plan

	STAKEHOLDER TYPE	DELIVERY METHOD
General Synod	Board	Letters / Reports
ACNC	Commonwealth Regulators	Letters / Reports / Online
Commonwealth Government	Commonwealth Regulators	Letters / Reports / Online
State Government	State Regulators	Letters / Reports / Online
Local Government	Local Government Regulators	Inspections
KPMG	Auditors	Letters / Meetings/ Email / Phone
WTW	Broker	Email / Phone
Insurers	Insurer	Via WTW
Public	Clients / Parishioners	Letter / Website
Public	Media	Press Release

DIOCESAN COUNCIL / THE PERTH DIOCESAN TRUSTEES POLICY 41

**Anglican
Church**
Diocese of Perth



Key Message Plan

STAKEHOLDER GROUP	MESSAGES	DELIVERY METHOD	BY WHO AND WHEN
Internal Staff	Mission, objectives, unity, compliance, roles and responsibilities, trust	Email, website, Messenger, Bulletin, LMS	Archbishop / Diocesan Secretary
Agencies, Schools and Commissions	Mission, objectives, unity, trust	Website, Messenger, Bulletin	Archbishop
Government	Good Governance	Letters / reports / online / website	Archbishop / Diocesan Secretary
Public	Community Relevance	website / media	Archbishop

DIOCESAN COUNCIL / THE PERTH DIOCESAN TRUSTEES POLICY 41

**Anglican
Church**
Diocese of Perth



Appendix G – Risk Register Template

Risk Details - Anglican Diocese of Perth

Risk Theme

--	--

Risk Owner

Date Reviewed

Risk Goal

--	--

Control Rating

Risk Rating

Event / Potential Threat / Inherent Risk				EVENTS OCCUR RISK	Impact / Consequence		Impact	Mitigating	Impact
Ref	Description	Preventative Controls	Likelihood		Ref	Description	Type	Controls	
E1					I1				
E2					I2				
E3					I3				
E4					I4				
E5					I5				
E6					I6				

Preventative Controls					
Ref	Description	Entity	Owner	Rating	Status
C1					
C2					
C3					
C4					
C5					
C6					

Mitigating Controls					
Ref	Description	Entity	Owner	Rating	Status
M1					
M2					
M3					
M4					
M5					
M6					

Owner Legend	



Appendix H – 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 financially viable, sustainable business model within the Church, governance framework and historical legacies.

3. Health and Safety

Inadequate health and safety 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. Includes the failure to protect information from cyber threats and privacy breaches.

6. Ministry / Service / Business Interruption

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

7. Commercial Asset and Property Management

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

8. 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.

9. Safe Ministry and 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 I – Controls Effectiveness Rating

RATING	SCORE	CRITERIA
EFFECTIVE	5	Control design is effective with no major control improvements required. Controls are effectively performed to design specification.
MOSTLY EFFECTIVE	4	Control design is satisfactory; however minor improvements have been identified. Controls are performing low levels for the design specification and need improvement.
PARTIALLY EFFECTIVE	3	Control design is satisfactory; however major improvements have been identified. Controls are performing below design specification and need major improvement.
LARGELY INEFFECTIVE	2	Controls have not been fully developed. The control is not performing as designed and the control system is largely ineffective.
NONE OR TOTALLY INEFFECTIVE	1	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design or very limited operational effectiveness.



Appendix J - Likelihood Criteria

LIKELIHOOD	RATING	DEFINITION
ALMOST CERTAIN	5	<p>The risk is expected to occur at least once in the next 12 months</p> <p>Less than 10% of the risk controls are Effective or Mostly Effective</p> <p>Without control improvement, it is almost certain this risk will eventuate at some point in the next 12 months.</p>
LIKELY	4	<p>There is a strong possibility that the risk will occur in the next 24 months</p> <p>Only 10-30% of the risk controls are Effective or Mostly Effective</p> <p>Without control improvement, it is more likely than not this risk will eventuate in the next 24 months</p>
POSSIBLE	3	<p>The risk might occur in the next 3 years</p> <p>30-70% of the risk controls are either Effective or Mostly Effective</p> <p>Without control improvement, the risk may eventuate in the next 3 years</p>
UNLIKELY	2	<p>There is a small possibility that the risk will occur in the next 3 years</p> <p>70-90% of the risk controls are rated Effective or Mostly Effective</p> <p>The strength of the internal controls means it is more likely the risk would eventuate caused by external factors</p>
RARE	1	<p>There is a remote possibility the risk will occur in 3-5 years</p> <p>90% or more of the risk controls are rated Effective or Mostly Effective</p> <p>The strength of the controls means that if the risk eventuates it is most likely result of external circumstances outside of the control of the organisation</p>



Appendix K – Consequence Criteria

	CONSEQUENCE / IMPACT				
CONSEQUENCE CATEGORY	INSIGNIFICANT	MINOR	MODERATE	MAJOR	CATASTROPHIC
	1	2	3	4	5
PEOPLE - HEALTH AND SAFETY	No injury / illness - no TLTI, minor adjustment to operational routine.	Single minor injury/ illness – TLTI < 4 Days	Single injury / illness requiring extended treatments. TLTI 4 to 10 Days.	Injury or Illness that requires immediate treatment as hospital in-patient. TLTI > 10 Days. Notifiable Incident	Fatality or multiple fatalities Notifiable Incident
PEOPLE - ABUSE AND NEGLECT	Single allegation or incident that requires local on-site review.	Single allegation, safeguarding system fault or incident that requires supervisor review and policy review.	Allegation, safeguarding system fault or incidents that require Immediate report to EO and /or external bodies.	Delay In Identifying abuse or neglect or a system fault requiring immediate EO report and independent review.	Multiple failures in safeguarding system that require immediate rectification, external review and external reporting.
PEOPLE –CHILD AND VULNERABLE PEOPLE SAFETY	Injuries requiring first aid or minor medical treatment only. Unlikely to require change to safety policy or systems	Minor harms requiring medical treatment and/or hospitalisation. Supervisor involvement and local review. Likely to require change to safety policy or system	Harms requiring external medical treatment and/or serious Incident reporting. Harms that involve two or more persons Supervisor involvement and management review. Will involve changes to safety policy and/or system	Harms impacting immediate safety of individuals requiring immediate removal from threat, immediate high-level care / treatment and Immediate reporting to EO and external bodies Immediate review of safety policy and system	Widespread harms or harms that result in threat to life, serious mental anguish and/ or permanent disability. Immediate EO intervention and reports to external bodies Immediate rectification of safety policy and systems.

**DIOCESAN COUNCIL /
THE PERTH DIOCESAN TRUSTEES
POLICY 41**

**Anglican
Church**
Diocese of Perth



	CONSEQUENCE / IMPACT				
CONSEQUENCE CATEGORY	INSIGNIFICANT	MINOR	MODERATE	MAJOR	CATASTROPHIC
	1	2	3	4	5
FINANCIAL - LOSS	< \$5,000	\$5,001 - \$50,000	\$50,001 - \$2,000,000	\$2,000,001 - \$20,000,000	> \$20,000,001
OPERATIONS - CYBER	No impact on systems	Minor impact resulting in no loss of services or additional costs	Some impact resulting in limited access to systems or files. Minor costs to rectify incurred	Considerable impact resulting in data breach, access to files or some systems. Moderate costs to rectify incurred Notifiable Privacy Incident	Severe impact resulting in system failure, no system access or denial of service. Substantial costs to rectify incurred
OPERATIONS - PROJECT DELIVERY	On track, on budget completion date at risk	< 1-month behind schedule and minor increase in cost (<10% over budget)	1-month behind schedule, moderate increase in costs (less than 11% - 20% over budget)	> 1-month behind schedule, significant increase in costs (more than 20% over budget)	Extreme increase in cost, disruption of schedule, or degradation of deliverable or discontinuation
OPERATIONS - QUALITY OF SERVICE	No impact on the quality of service	Minor impact on the quality of services resulting in an increase in complaints from the community or stakeholders (<10%)	Moderate impacts on the quality of services resulting in an increase in complaints from the community or stakeholders (10%-25%)	Considerable impact on the quality of services resulting in a marked increase in complaints from the community or stakeholders (25% -50%)	Severe impact on the quality of service provided resulting in significant increase in complaints or incidents (>50%)

**DIOCESAN COUNCIL /
THE PERTH DIOCESAN TRUSTEES
POLICY 41**

**Anglican
Church**
Diocese of Perth



	CONSEQUENCE / IMPACT				
CONSEQUENCE CATEGORY	INSIGNIFICANT	MINOR	MODERATE	MAJOR	CATASTROPHIC
	1	2	3	4	5
OPERATIONS - BUILDING AND PROPERTY	No impact to building and property	Minor impact resulting in no loss of operations or additional costs	Some impact resulting in limited access to building and/or property. Minor costs to rectify incurred	Considerable impact resulting in loss of access to or damage to some building and property. Some impact on business operations Moderate costs to rectify incurred	Severe impact resulting in loss of building and property with business operations impacted. Substantial costs to rectify incurred
REPUTATION	External reputation not damaged	External reputation minimally affected. Little effort or expense to recover. Minor impact on staff turnover increase of 5% -10% of staffing levels.	External reputation impacted requiring some expense to recover. Moderate impact on staff turnover increase of 10% -20% of staffing levels	External reputation severely impacted requiring considerable effort and expense to recover. Major impact on staff turnover increase of 20% - 32%) of staffing levels	External reputation permanently damaged. Severe impact on staff turnover > 33% of staffing levels
LEGAL AND COMPLIANCE	Compliance with standards or legal requirements maintained with negligible level of control weakness.	Compliant with standards or legal requirements, but with some minor level of control weakness needing attention.	Single noncompliance with standards or legal requirements resulting in recommendations for improvement / moderate level of control weakness identified.	Multiple non compliances with standards or legal requirements resulting in urgent improvements / high level of control weakness.	Fully non-compliant with standards or legal requirements resulting in sanction or penalty / critical failure of key controls



Appendix L – Risk Rating Matrix

	CONSEQUENCE / IMPACT					
		INSIGNIFICANT 1	MINOR 2	MODERATE 3	MAJOR 4	CATASTROPHIC 5
LIKELIHOOD	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)	Low (6)	Medium (9)	High (12)	High (15)
	UNLIKELY 2	Very Low (2)	Low (4)	Low (6)	Medium (8)	High (10)
	RARE 1	Very Low (1)	Very Low (2)	Low (3)	Low (4)	Medium (5)